

HiPath 2000 V1.0

Systembeschreibung

SIEMENS

Global network of innovation

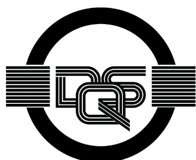


1P P31003-E1010-X200-6-18

Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden. Die verwendeten Marken sind Eigentum der Siemens Enterprise Communications GmbH & Co. KG bzw. der jeweiligen Inhaber.



Die Konformität des Gerätes zu der EU-Richtlinie 1999/5/EG wird durch das CE-Kennzeichen bestätigt.



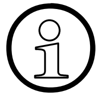
Dieses Gerät wurde nach unserem zertifizierten Umweltmanagementsystem (ISO 14001) hergestellt. Dieser Prozess stellt die Minimierung des Primärrohstoff- und des Energieverbrauchs sowie der Abfallmenge sicher.

Hofmannstraße 51, D-81359 München
Bestell-Nr.: P31003-E1010-X200-6-18
Liefermöglichkeiten und technische Änderungen vorbehalten.

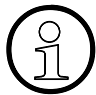
Inhalt

1 Einleitung

Dieses Dokument beschreibt den Leistungsumfang der HiPath 2000 V1.0 und ihre Schnittstellen.



Mit dieser Systembeschreibung ist die Leistungsmerkmalbeschreibung und Vertriebsinformation (https://netinfo.icn.siemens.de/es/products/prod_hipath_3000_edge_v1_0/product/vf_doku/sales_info) verknüpft.



Die verfügbaren Leistungsmerkmale und die freigegebenen Anwendungen können sich von Land zu Land unterscheiden.
Die Vertriebsinformation ist deshalb das einzige Dokument, welches verbindlich die verfügbaren Leistungsmerkmale und den Hardwareumfang für Ihr Land beschreibt.

1.1 Übersicht über HiPath 2000 V1.0

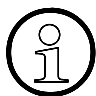
Einführung in die HiPath 2000-Systeme

HiPath 2000 ist eine reine IP-Plattform, die als selbstständiges IP-Kommunikationssystem (Standalone) oder als Filiallösung (Branch) für HiPath 3000, HiPath 4000 und HiPath 5000 eingesetzt werden kann.

HiPath 2000 kombiniert modernste IP-Routerfunktionalität mit dem vollen HiPath ComScendo-Sprachleistungsumfang in einem einzigen System. Integrierte Funktionen wie Router, Gateway und Firewall schaffen die Voraussetzungen für eine gesicherte IP-Kommunikation in Virtual Private Networks VPN.

Kleinen und mittleren Unternehmen wird damit der Weg zu modernster IP-Kommunikation für Daten und Sprache über eine einheitliche Infrastruktur eröffnet. Unternehmen, die bereits heute konsequent auf durchgängige IP-Technologie setzen, bietet HiPath 2000 einen Zugang zu ITSPs (Internet Telephony Service Provider) für DSL-Telefonie.

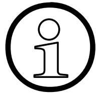
Diese Systembeschreibung beinhaltet Informationen zu allen HiPath 2000-Systemen und deren Varianten. Angaben zur Vermarktung der einzelnen Varianten in den verschiedenen Ländern sind bei den zuständigen Stellen einzuholen.



Hipath 2000 ist als "Inhouse System" konzipiert. Sollten Leitungen angeschlossen werden, die das Gebäude verlassen oder eine Länge von 500m überschreiten (z.B. bei sehr grossen oder hohen Gebäudekomplexen möglich), so ist ein zusätzlicher Überspannungsschutz (Primär- oder Sekundärschutz) erforderlich. Details dazu finden sie im Servicehandbuch Kapitel 3.

Als Teilnehmer-Schnittstellen werden IP-Workpoints und Clients mit HiPath ComScendo-Leistungsmerkmalen unterstützt.

	HiPath 2020 Branch (Filiallösung)	**HiPath 2030 Standalonelösung**
Workpoints	• Maximal 20 IP-Workpoints	• Maximal 30 IP-Workpoints
Hardware-Modelle	• Welt = 2 x S_0 (optional als Teilnehmer oder Amt einrichtbar) • USA = 1 x T1	• Welt = 4 x S_0 (optional als Teilnehmer oder Amt einrichtbar) • USA = 1 x T1
	• 4 Port LAN Switch • 1 x WAN • 1 x DMZ • 1 x USB (für Servicezwecke)	• 4 Port LAN Switch • 1 x WAN • 1 x DMZ • 1 x USB (für Servicezwecke) • 2 x a/b (für den Teilnehmeranschluss)
Integrierte Voice Mail	nicht verfügbar	• 2 Sprachkanäle • bis zu 24 Mailboxen • Aufnahmekapazität bis 120 Minuten • 2 separate Begrüßungen pro Mailbox • 4 x AutoAttendant mit Begrüßungen und Anrufvermittlung • Kurzwahlziele pro Auto-Attendant einstellbar
Aufbauvarianten	Tisch-/Wand- und 19”-Aufbau, Platzbedarf im 19“-Rack = 1 Höheneinheit	
Abmessungen	Breite = 440 mm (478 mm einschließlich Gehäusefüße) Höhe = 44 mm (55 mm einschließlich Gehäusefüße) Tiefe = 240 mm	
Unterbrechungsfreie Stromversorgung USV	extern (keine Bestellposition)	
Farbe	Stahlblau / Arcticgrau	Stahlblau / Arcticgrau



DMZ

DMZ (**Dem**ilitarisierten **Z**one) bedeutet, dass zwei physikalisch getrennte Firewalls vorhanden sind. HiPath 2000 besitzt ausschließlich **eine** zentrale Firewall.
Dient dem Anschluss von E-Mail-Servern, Web-Servern und WLAN Access Points mit folgenden Randbedingungen:

- Festlegung eines eigenen IP-Adressbereichs
- Separate physikalische LAN-Schnittstelle, abgesichert über die Firewall des Systems

Die DMZ verhindert somit Zugriffe von außen auf interne IT-Strukturen.

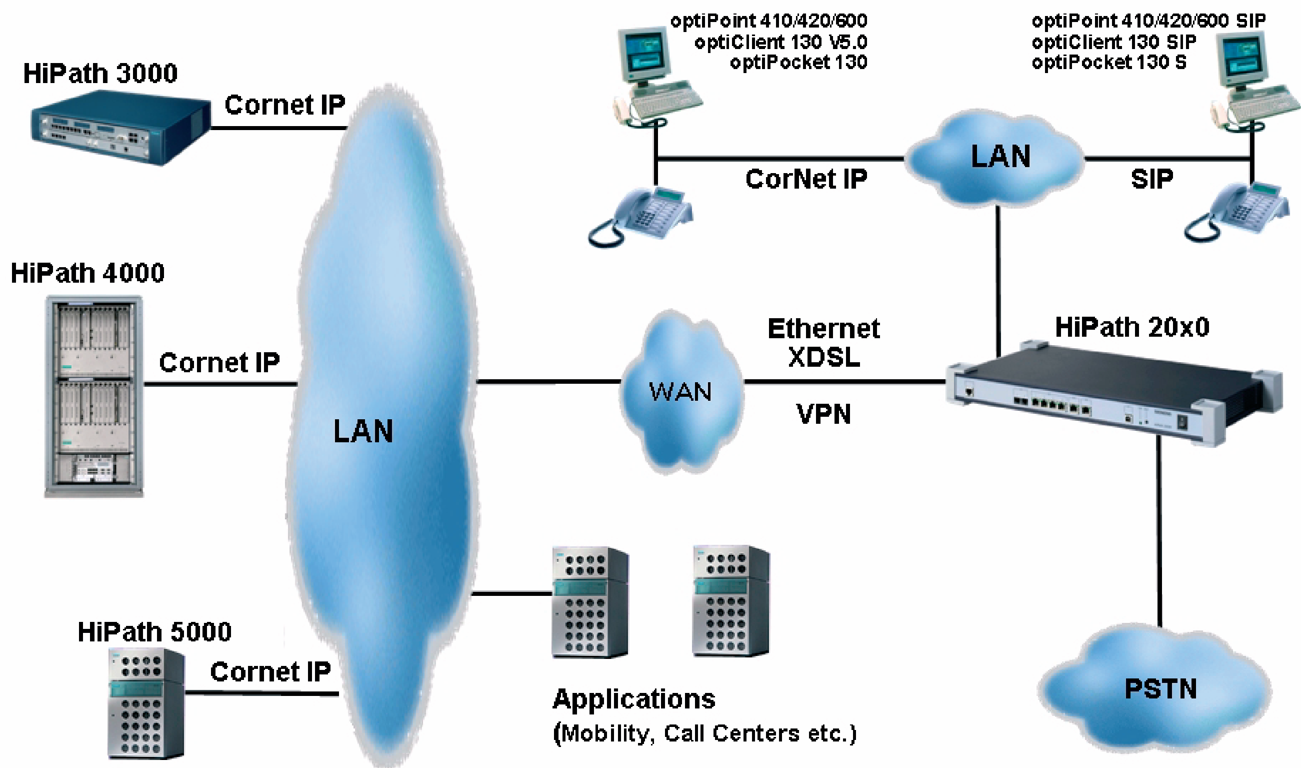
1.2 Systemvarianten HiPath 2020 und HiPath 2030

1.2.1 HiPath 2020

HiPath 2020 unterstützt den Anschluss von maximal 20 IP-Workpoints und wird vorrangig als kleine Filiallösung (Branch) für HiPath 3000, HiPath 4000 und HiPath 5000 eingesetzt.

Die Versorgung des Systems erfolgt über eine integrierte Stromversorgung.

Das Bild zeigt ein Beispiel als Networked Szenario in HiPath-Netzen



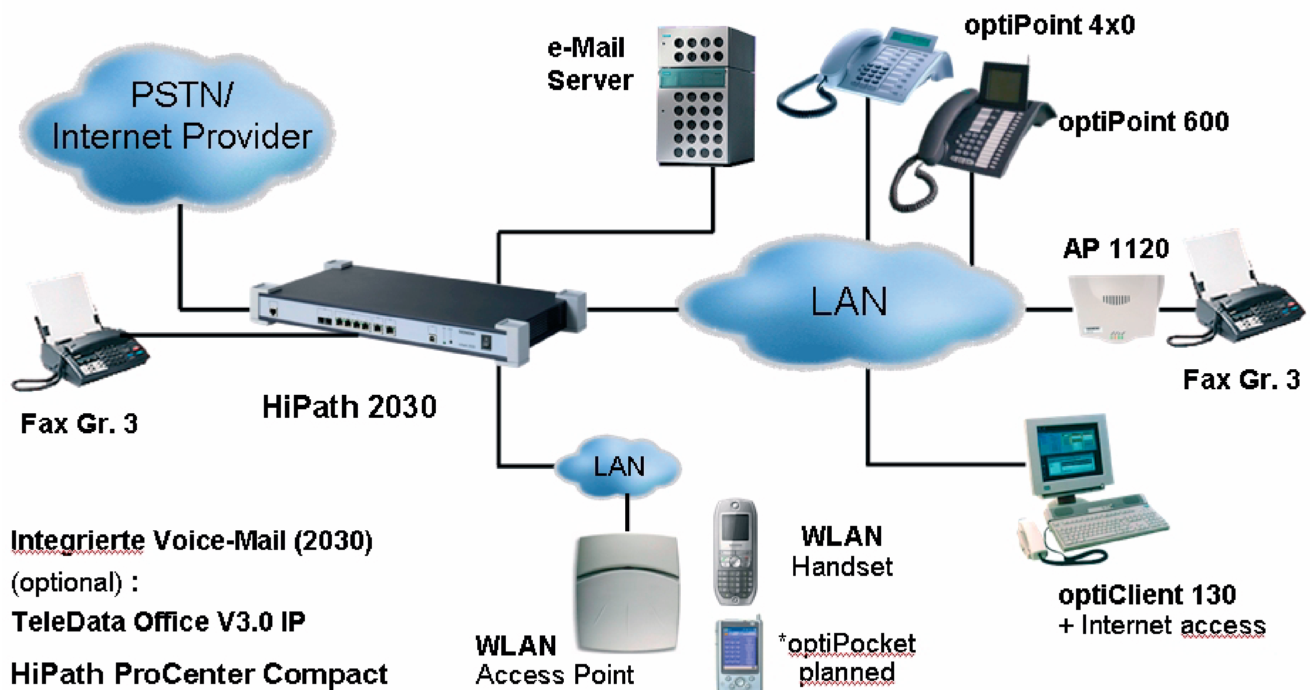
1.2.2 HiPath 2030

HiPath 2030 unterstützt den Anschluss von maximal 30 IP-Workpoints und wird vorrangig als selbstständiges IP-Kommunikationssystem (Standalone) eingesetzt. Zusätzlich bestehen Anschlussmöglichkeiten für zwei analoge Endgeräte und ISDN-Endgeräte (nur HiPath 2030-Variante S_0).

Darüber hinaus ist HiPath 2030 standardmäßig mit der integrierten Voice Mail ausgestattet. Eine Gegenüberstellung von der Integrierte Voice Mail zur HiPath Xressions Compact finden Sie in der Leistungsmerkmalbeschreibung.

Die Versorgung des Systems erfolgt über eine integrierte Stromversorgung.

Das Bild zeigt ein Beispiel als Standalone Szenario



1.3 Highlights des neuen Produktes

Das IP-System HiPath 2000 bietet kleinen mittelständischen Unternehmen zuverlässigste Sprachkommunikation mit hochwertigen Endgeräten bei einfachster Bedienung.

- Neues IP-System mit dem Betriebssystem LINUX
- Zwei Systemvarianten: HiPath 2020 und HiPath 2030 für den Einsatz als Standalone-System und als Filial-System in Netzen
- Integrierte Netzwerkkomponenten für Daten und Sprache, wie Router, Firewall, DMZ, LAN-Switch
- Voller HiPath ComScendo-Leistungsumfang
- Einsatz in Filiallösung gemeinsam mit HiPath 3000/HiPath 4000/HiPath 5000 (CorNet-IP)
- SIP-Unterstützung für SIP-Endgeräte
- SIP-Unterstützung für den Anschluss an Internet Telephony Service Provider
  - DSL-Telefonie-Teilnehmeranschluss für die Registrierung von Einzelrufnummern
  - DSL-Telefonie-Anlagenanschluss für die Registrierung von Rufnummernband
- Integrierte Voice Mail (HiPath 2030), Music-on-hold mit individuellen Ansagen
- optiPoint 410/420, optiClient, WLAN-Ausrüstung
- HiPath End-to-End-Lösung für VoWLAN mit optiPoint WL2 professional und HiPath Wireless Standalone Access Point WL AP 2630 oder WL AP 2640
- Web-based Management WBM für Administration, Lizenzierung und Wartung

1.3.1 Übersicht der Leistungsmerkmale

In den folgenden Tabellen sind die Leistungsmerkmale der HiPath 2000 V1.0 dargestellt und kurz erläutert:

Systemarchitektur

Leistungsmerkmal	Erläuterung
Hardware	**Ausbau** An HiPath 2020 und HiPath 2030 werden im Festausbau geliefert. **Montagemöglichkeiten** ● Wandinstallation ● Tischaufstellung ● Einbau in 19"-Standardschränke. Keine Zusatzkühlung erforderlich.
Betriebssystem	Das Betriebssystem der HiPath 2000 V1.0 ist Linux. Die Siemens Enterprise Communications GmbH & Co. KG ist verpflichtet, die verwendeten Open Source-Anteile zu benennen und zu veröffentlichen. Alle Informationen dazu finden Sie auf der System CD.
IP-Workpoints	● HiPath 2020: maximal 20 IP-Workpoints ● HiPath 2030: maximal 30 IP-Workpoints

Leistungsmerkmal	Erläuterung
Integrierte Voice Mail	Nur die Anlagenvariante HiPath 2030 verfügt über die integrierte Voice Mail-Funktion mit folgenden Funktionen: ● 2 Sprachkanäle ● 24 Mailboxen, davon 4 als AutoAttendant ● 2 verschiedene persönliche Begrüßungen von je einer Minute Dauer, die manuell oder per Nachtschaltung aktiviert werden. ● Aufnahmekapazität bis zu zwei Stunden oder maximal 400 Nachrichten/Begrüßungen. Die Dauer der einzelnen Sprachnachrichten kann in Minutenschritten von einer bis 5 Minuten eingestellt werden. An jede gespeicherte Nachricht werden ein Zeitstempel und die Anrufer-ID angehängt. ● AutoAttendant-Funktionen: – Der Anrufer erhält eine maximal zweiminütige Begrüßung und hat dann die Möglichkeit mittels Sprachmenü Kontaktpersonen auszuwählen (maximal 10) oder die Durchwahlnummer einzugeben. – Automatische Rufweiterleitung zum Überlaufplatz – Faxtonerkennung und Faxweiterleitung ● Ansagen: – Selektion eines Kanals oder beider Kanäle für den Betrieb des Ansagegerätes

Alle relevanten Informationen finden Sie auf der System CD und unter folgender Adresse:
https://netinfo.icn.siemens.de/es/products/prod_hipath_3000_edge_v1_0/product/vf_doku/sales_info

Leistungsmerkmale

Leistungsmerkmal	Erläuterung
Integrierte Router-Funktion (Network Address Translation/Port Address Translation)	HiPath 2000 verfügt über eine integrierte DSL-Routerfunktion für folgende Funktionen: ● DSL-Protokolle PPPoE und PPTP ● ADSL (Asymmetric DSL) und SDSL (Symmetric DSL) Für die Anschaltung ist ein externes DSL-Modem erforderlich. (nicht im Lieferumfang der HiPath 2000). Dies wird im Regelfall durch den Provider bereitgestellt.

Leistungsmerkmal	Erläuterung
Firewall Funktion	Hipath 2000 schützt das Kundennetz durch integrierte Firewall-funktionen mit folgende Leistungsmerkmalen: ● Rufnummern-Überprüfung (nur kommend) ● Rückruf ● Prüfung von Benutzerkennung und Passwort ● Firewall (Erlaubnis-Firewall) ● Network Address Translation (NAT) ● Simple Traversal of UDP over NATs (STUN)
DHCP Server/Client DNS Client DLI (Integrierte Deployment Licence Service Funktion)	Integrierte DHCP-Server/Client, DNS Client und DLI-Funktionen mit folgenden Leistungsmerkmalen: ● DHCP Server für die Versorgung von IP-Workpoints und anderen Servern mit IP-Adressen ● DHCP Client für die Unterstützung externer DHCP-Server ● DNS Client für die Namesauflösung ● DLI Funktion zur automatische Inbetriebnahme von optiPoint 410/420 (HFA), optiPoint 600, WL2 Professional (HFA) und optiClient 130 sowie für den Software-Update für 410/420 (HFA) und WL2 Professional (HFA) Möchte der Kunde einen eigenen DHCP-Server nutzen, kann der systeminterne DHCP-Server deaktiviert werden.

Leistungsmerkmal	Erläuterung
Virtual Private Network (VPN)	Durch Virtual Private Networks (VPN) und IPSec erhöht sich die Sicherheit bei der Site-to-Site Standortvernetzung mit folgenden Vorteilen: ● Sichere Verbindung über Internet, keine Manipulation der vertraulichen Sprach und Datenkommunikation ● Sichere Integration von externen Partnern ins Firmennetz ● Zugriff auf Unternehmensinformationen für den Außendienst (Teleworker) VPN nutzt die öffentliche Infrastruktur des Internets. Durch IPSec-Verschlüsselungs- und Authentifizierungsmechanismen wird erreicht, dass Standortvernetzungen, Zugänge für Teleworker und das Einbeziehen von externen Partnern in den Kommunikationsfluss des Unternehmens gegen Zugriffe von außen gesichert und damit "privat" sind. **Vernetzungsarten:** ● Site-to-Site VPN (Standortvernetzung) ● Remote Access VPN (Fernzugriff von mobilen Mitarbeitern) **Leistungsmerkmale:** ● IPSec: Authentifizierung und Vertraulichkeit mittels ESP ● Lizenzierung der IPSec-Verschlüsselungsmechanismen der integrierten Light Weight Certification Authority ● Tunneling, gesicherte VPN-Verbindung zu einem anderen VPN-Gateway oder einem VPN-Client ● Anbindung von Teleworkern an das VPN (Safenet Sentinel) ● Automatic Reconnect (automatischer Wiederaufbau der Internetverbindungen nach der Zwangstrennung) Hinweis: Einschränkungen der VPN-Funktionalität finden Sie in der Systembeschreibung.
ComScendo	Voller ComScendo Sprachleistungsmerkmalumfang
Web-based Management (WBM)	HiPath 2000 bietet integrierte Managemementfunktionen für die Einrichtung und Wartung. Der Zugang zum System erfolgt über den Standard Microsoft Internet Explorer.
Session Initiation Protocol (SIP)	Das SIP-Protokoll ermöglicht den Anschluss von SIP-Telefonen wie optiPoint 410/420 S oder Standard-SIP-Endgeräte und die Anbindung an ITSP für die künftige Internettelefonie.
Virtual Local Area Network (VLAN)	HiPath 2000 unterstützt VLAN gemäß 802.1Q

Leistungsmerkmal	Erläuterung
CorNet-IP Interworking	Vernetzungen mit HiPath 2000 Systemen untereinander oder mit HiPath 3000/4000/5000 werden über das CorNet-IP Interworking inklusive Small Remote Sites-Szenarien unterstützt.
Applikationsschnittstellen	Für die Anbindung von Applikationen werden folgende Schnittstellen unterstützt: SNMP Version 1, DDE, TAPI, JTAPI, CSTA asn.1, CSTA XML
Service Remote Access	Der Fernzugriff für Service erfolgt über IP

Leistungsmerkmale für die Sprachübertragung

Leistungsmerkmal	Erläuterung
QoS (Quality of Service)	Die Sprachqualität im IP-Netz wird mit folgenden QoS-Protokollen sichergestellt: ● IEEE802.1p Tags (Ebene 2) ● Type of Service (ToS) Priorisierung (RFC 791, Ebene 3) ● Differentiated Services (DiffServ; RFC 2474, Ebene 3)
CODECs	Folgende CODECs werden durch HiPath 2000 unterstützt: ● G.711 a-law; High Quality ● G.711 µ-law, High Quality ● G.729 A/B, Low Bandwidth, good quality ● G.729 A, Low Bandwidth, good quality ● G.723, Lowest Bandwidth, fare quality Die optiPoint 410/420 Familie (HFA- und SIP-Variante) unterstützen alle o.g. CODECs. optiPoint 600 office unterstützt ausschließlich G.711 und G.723.
Echounterdrückung (Echo Cancelation)	HiPath 2000 unterstützt Echounterdrückung nach G.168
Sprechpausenerkennung (VAD, Voice activity detection),	Bei Sprechpausen wird für alle unterstützten CODECs in beide Richtungen ein Hintergrundrauschen übertragen, um das Verhalten traditioneller Telefonleitungen zu emulieren.
Fax über IP, Modem über IP	HiPath 2000 unterstützt den Betrieb von analogen Faxgeräten oder Modems in IP Netzen ● Fax über IP: – transparente G.711-Gateway-Kanäle – T.38-Kanäle: T.38 bietet zwar die zuverlässigere Übertragungsmethode, kann aber nur bis maximal 14 kBit/s genutzt werden. ● Modem über IP: – transparente G.711-Gateway-Kanäle

Leistungsmerkmal	**Erläuterung**
DTMF-Behandlung	Erkennung und Behandlung von DTMF-Signalen entspr. Q.24 zur Signalisierung bei VoIP-Gesprächen. Unterstützung der folgenden Funktionen: ● Erkennung von DTMF-Zeichen ● Umwandlung von DTMF-Zeichen in Benutzereingabesignale nach H.245 ● Erzeugung von DTMF-Zeichen für das PSTN ● Sprachschutz unter Verwendung von Bellcore-Testbändern

Nähere Informationen finden Sie in der Leistungsmerkmalbeschreibung HiPath 2000 V1.0:

- Deutsch/Englisch: https://intranet.com.siemens.de/techdoc

1.3.1.1 Kundennutzen

1.3.1.1.1 Alleinstellungsmerkmale (Unique Selling Proposition)

- HiPath 2000 V1.0 integriert in einem System:
  - IP-Kommunikation mit vollem ComScendo-Leistungsumfang in einer IP-Infrastruktur
  - Router-Funktion mit 4-Port-LAN-Switch und DMZ-Anschluss
- Offene Architektur durch Linux-basiertes IP-System mit umfassendem Leistungsmerkmalangebot und Endgeräten inklusive des SIP-Standards
- Hohe Verfügbarkeit und Ausfallsicherheit im "Hosted" Lösungs-Umfeld

1.3.1.1.2 Betrachtung von Nutzen und Wirtschaftlichkeit

Die Plattform HiPath 2000 V1.0 bietet flexibel und kostenoptimiert zuverlässigste und komfortable IP-Kommunikation. Dadurch kann sie, besonders in mittelständischen und großen Unternehmen, wesentlich zur Steigerung der Produktivität beitragen.

Sie ist ein zukunftssicheres IP-System, das die nötige Flexibilität für Veränderungen in der IP-Technologie aufweist.

Flexibel:

- HiPath 2000 V1.0 stellt für alle Kommunikationsprozesse an jedem Arbeitsplatz und in jedem Arbeitsumfeld umfangreiche Kommunikationsleistungsmerkmale und die passenden Applikationen zur Verfügung. Dies ist unabhängig von:
  - dem verwendeten IP-Netz
  - den verwendeten Workpoints (IP, a/b, DECT, WLAN oder PC-Clients)

- Die breite Palette an Endgeräten und PC-Clients bietet für jeden Arbeitsplatz das optimale Telefon.
- Einfache Anbindung von Filialen und Teleworkern
- Bereitstellung des Internetzugangs durch integrierte Router-Funktion
- Flexible Erweiterungen über Lizenzen
- Offen für zukünftige ITSP Services

Kostenoptimiert (CAPEX/OPEX/TCO):

- Geringe Anschaffungskosten
- Leistungsabstufung der Endgeräte. Kostenoptimierte Arbeitsplatzausstattung.
- Wirtschaftliche Filialkonzepte für kleine Filialen ohne Verzicht auf Leistungsmerkmale und leistungsstarke Applikationen
- Kosteneinsparungen durch bessere Nutzung zentral bereitgestellter Applikationen
- Schnelle Inbetriebnahme mit Standardfunktionen durch vorkonfigurierte Systeme
- Servicefreundlichkeit des Systems durch einfache Administration und Remote-Zugänge

Zuverlässig:

Gewährleistung der Zuverlässigkeit der IP-Telefonie

Komfortabel:

- Hoher Sprachkomfort
- Voller ComScendo-Leistungsumfang
- Administration über integriertes Web-based Management
- Gesicherte IP-Kommunikation durch IPSec-VPN
- Homogene Leistungsmerkmale und Applikationen werden plattformübergreifend bei der Vernetzung mit HiPath 3000, 4000 und 5000 bereitgestellt.

1.3.2 DSL-Telefonie

HiPath 2000 unterstützt die Anbindung an Internet Telephonie Service Provider (ITSP) und damit die Nutzung der DSL-Telefonie.

Hinweis: Der in dieser Dokumentation verwendete Begriff DSL-Telefonie bezieht sich auf das Telefonieren über IP-gestützte Netze (Voice over IP) und eine Signalisierung mittels SIP-Protokoll.
Das SIP-Protokoll (Session Initiation Protocol) ist ein ASCII-basierendes Signalprotokoll, dass zur Einrichtung von Sitzungen in einem IP-Netz verwendet wird.

1.3.2.1 DSL-Telefonie-Teilnehmer

Folgende Workpoints werden unterstützt:

- optiPoint 410 S
- optiPoint 420 S
- optiPoint 150 S

1.3.2.2 DSL-Telefonie-Leistungsmerkmale

Folgende Leistungsmerkmale für DSL-Telefonie-Teilnehmer werden aktiv unterstützt:

- CLIP (Anzeige der Rufnummer des rufenden Teilnehmers beim gerufenen Teilnehmer)
- CLIR (Unterdrückung der Rufnummernanzeige des rufenden Teilnehmers beim gerufenen Teilnehmer)
- COLP (Anzeige der Rufnummer des gerufenen Teilnehmers beim rufenden Teilnehmer)
- COLR (Unterdrückung der Rufnummernanzeige des gerufenen Teilnehmers beim rufenden Teilnehmer)
- Rückfrage
- Übergabe
- Halten
- Übergeben nach Melden (Call Transfer)

Folgende Leistungsmerkmale können DSL-Telefonie-Teilnehmer zwar nicht aktivieren, sie können allerdings passiv eingebunden werden:

- Anrufumleitung (Umleitung auf einen DSL-Telefonie-Teilnehmer wird unterstützt.)
- Konferenz (DSL-Telefonie-Teilnehmer kann passiv eingebunden werden.)

- Parken (DSL-Telefonie-Teilnehmer können geparkt werden. Aus Sicht des DSL-Telefonie-Teilnehmers ist dies wie “Halten”.)
- Live Call Recording (DSL-Telefonie-Teilnehmer kann passiv eingebunden werden.)
- Diskretes Ansprechen (DSL-Telefonie-Teilnehmer kann passiv eingebunden werden.)
- Übergeben vor Melden (Übergeben vor Melden auf einen DSL-Telefonie-Teilnehmer ist möglich.)

Native SIP unterstützt ausschließlich:

- Basic Call
- Halten
- Rückfrage

1.4 Lizenzierung

Die Verwaltung und Freischaltung der HiPath 2000 V1.0 Lizenzen erfolgt über HiPath License Management (HLM) nach dem bei HiPath 3000 ab V5.0 eingeführten Verfahren.

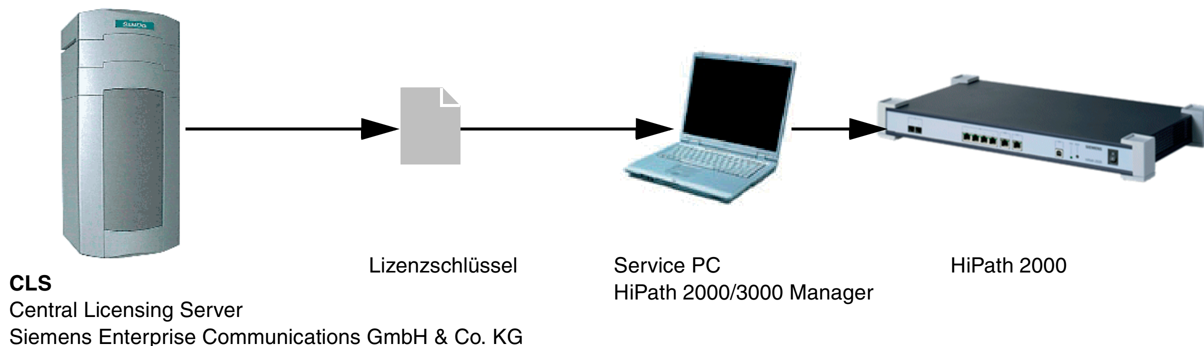
Die Lizenierung ist für den Betrieb der Anlage zwingend erforderlich.

Innerhalb der Grace Period (30 Tage, uneingeschränkter Betrieb) muss ein gültiges Lizenzfile eingebracht werden, eingeschränkter Notbetrieb (mit einem IP-User und Fernverwaltung) ist immer sichergestellt.

1.4.1 HiPath License Management

Das HiPath License Management ist ein zentralisiertes Verfahren zur Verwaltung von Lizenzen. Auf Basis der Bestelldaten kann über den Central Licensing Server (CLS) ein Lizenzschlüssel für eine Lizenzposition bezogen werden.

Die Customer Site Komponenten CLC und CLA sind bei der HiPath 2000 im System integriert. Mit Hilfe des CLM werden die Lizenzen der HiPath 2000 übergeben.



Zur Nutzung des Systems sind folgende Lizenzen zwingend erforderlich:

- HiPath 2000 V1.0-Systemlizenz (ist eine immer erforderliche Vermarktungsposition, bestehend aus Systemlizenz + 10 ComScendo-Lizenzen für IP-Workpoints)
- HiPath 2000 V1.0-ComScendo-Erweiterungslizenzen für IP-Workpoints (optional)
- HiPath 2000 V1.0-IPSec-Lizenz (optional)
- HiPath 2000 V1.0-LWCA (Light Weight Certification Authority)-Lizenz (optional)
- HiPath 2000 V1.0-optiClient attendant V7.0-Lizenz (optional)
- HiPath TAPI 120 V2.0 (optional)
- HiPath CAP V3.0 (optional)

Die oben genannten HiPath 2000-Lizenzen können ausschließlich in HiPath 2000-Systemen verwendet werden. Die Lizenzen werden den Anlagen fest zugeordnet und sind nicht übertragbar auf andere Systeme.

Informationen über Lizenzpositionen der anschließbaren Applikationen und IP Clients entnehmen Sie bitte den entsprechenden Vertriebsinformationen.

1.5 Vertriebsunterstützende Unterlagen

- Lagerort und Bestellweg für folgende Artikel:

  Deutsch und Englisch im Lieferzentrum Fürth
  Fax: +49 911 654 4271
  Mail: lzf@znnbg.siemens.de
  Intranet: https://intranet.click4business-supplies.siemens.de

  – Bestellweg für Lieferzentrum Fürth
    https://www.click4business-supplies.siemens.de

- Andere Sprachen und Adressen
  siehe Verzeichnis der Lagerorte im Intranet:
  http://intranet.communications.siemens.de/vz_dc_2/lagerort.htm

Unterlage	Sprachen	Bestell-Nr.
Datenblätter Der Internet-Zugriff auf Datenblätter ist möglich über http://www.siemens.de/enterprise (–> Downloads)		
HiPath 2000 V1.0	Deutsch, Englisch	A31002-E1010-A100-*-29 A31002-E1010-A100-*-7629
HiPath 3000 V6.0	Deutsch, Englisch	A31002-H1000-A600-*-29 A31002-H1000-A600-*-7629
HiPath 4000 V3.0	Deutsch, Englisch	A31002-H3130-D100-*-29 A31002-H3130-D100-*-7629
HiPath 5000 V6.0	Deutsch, Englisch	A31002-H5000-A500-*-29 A31002-H5000-A500-*-7629
HiPath Manager E	Deutsch, Englisch	
HiPath Accounting Management	Deutsch, Englisch	A31002-H4100-A100-*-29 A31002-H4100-A100-*-7629
HiPath ComAssistant	Deutsch, Englisch	A31002-X7000-A230-*-29 A31002-X7000-A230-*-7629
HiPath Common Application Platform CAP V3.0	Deutsch, Englisch	A31002-X7000-A300-*-29 A31002-X7000-A300-*-7629
HiPath cordless	Deutsch, Englisch	A31002-G2100-A140-*-29 A31002-G2100-A140-*-7629
HiPath Fault Management	Deutsch, Englisch	A31002-G6900-A110-*-29 A31002-G6900-A110-*-7629
HiPath Simply Phone for Outlook 3.1	Deutsch, Englisch	A31002-X7000-A210-*-29 A31002-X7000-A210-*-7629
HiPath Simply Phone for Notes 3.1	Deutsch, Englisch	A31002-X7000-A200-*-29 A31002-X7000-A200-*-7629

Unterlage	Sprachen	Bestell-Nr.
HiPath TAPI 120	Deutsch, Englisch	A31002-E1300-A260-*-29 A31002-E1300-A260-*-7629
HiPath Xpressions	Deutsch, Englisch	A31002-S2300-A100-*-29 A31002-S2300-A100-*-7629
optiClient 130 V5.0	Deutsch, Englisch	A31002-A2000-B400-*-29 A31002-A2000-B400-*-7629
optiClient Attendant	Deutsch, Englisch	A31002-E1300-A320-*-29 A31002-E1300-A320-*-7629
optiPoint Attendant	Deutsch, Englisch	
optiPoint 410 family	Deutsch, Englisch	A31002-H1000-A500-*-29 A31002-H1000-A500-*-7629
optiPoint 420 family	Deutsch, Englisch	A31002-H1000-A520-*-29 A31002-H1000-A520-*-7629
optiPoint 410/420 S	Deutsch, Englisch	A31002-H1000-A850-*-29 A31002-H1000-A850-*-7629
optiPoint 600 office	Deutsch, Englisch	A31002-H1000-A260-*-29 A31002-H1000-A260-1*-7629
optiPoint WL2 professional / WL2 professional S	Deutsch, Englisch	A31002-J5000-A200-*-29 A31002-J5000-A200-*-7629
Teledata Office V3.0	Deutsch, Englisch	A31002-E1300-A270-*-29 A31002-E1300-A270-*-7629
Werbeschriften und -artikel Wenden Sie sich an Siemens Enterprise Communications GmbH & Co. KG Produkt Promotion.		

1.6 Technische Unterlagen

Auswahl und Download-Möglichkeit (HTML und PDF) von:

- Bediendokumentation
- Administratordokumentation
- Servicedokumentation
- Vertriebsdokumentation

finden Sie unter dem der folgenden Webseite:

https://netinfo2.icn.siemens.de/techdoc

1.7 Datenschutz und Datensicherheit

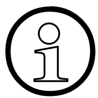
Umgang mit personenbezogenen Daten

Beim vorliegenden System werden u. a. personenbezogene Daten verarbeitet und genutzt, z.B. bei der Gebührenerfassung, den Displayanzeigen, der Kundendatenerfassung.

In Deutschland gelten für die Verarbeitung und Nutzung solcher personenbezogenen Daten u.a. die Bestimmungen des Bundesdatenschutzgesetzes (BDSG). Für andere Länder beachten Sie bitte die jeweiligen entsprechenden Landesgesetze.

Datenschutz hat die Aufgabe, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Ferner hat Datenschutz die Aufgabe, durch den Schutz der Daten vor Missbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener schutzwürdiger Belange zu begegnen.



Der Kunde ist dafür verantwortlich, dass das System in Übereinstimmung mit dem jeweils gültigen Datenschutz-, Arbeits- und Arbeitsschutzrecht installiert, betrieben und gewartet wird.

Mitarbeiter der Siemens Enterprise Communications GmbH & Co. KG sind durch die Arbeitsordnung zur Wahrung von Geschäfts- und Datengeheimnissen verpflichtet.

Um die gesetzlichen Bestimmungen beim Service – ob beim „Service vor Ort“ oder beim „Teleservice“ – konsequent einzuhalten, sollten Sie folgende Regeln unbedingt befolgen. Sie wahren damit nicht nur die Interessen Ihrer/unserer Kunden, sondern vermeiden dadurch auch persönliche Konsequenzen.

Richtlinien zum Umgang mit Daten

Tragen Sie durch problembewusstes Handeln mit zur Gewährleistung des Datenschutzes und der Datensicherheit bei:

- Achten Sie darauf, dass nur berechtigte Personen Zugriff auf Kundendaten haben.
- Nutzen Sie alle Möglichkeiten der Passwortvergabe konsequent aus; geben Sie keinem Unberechtigten Kenntnis der Passwörter, z.B. per Notizzettel.
- Achten Sie mit darauf, dass kein Unberechtigter in irgendeiner Weise Kundendaten verarbeiten (speichern, verändern, übermitteln, sperren, löschen) oder nutzen kann.
- Verhindern Sie, dass Unbefugte Zugriff auf Datenträger haben, z.B. auf Sicherungskopien oder Protokolldrucke. Das gilt sowohl für den Serviceeinsatz, als auch für Lagerung und Transport.

- Sorgen Sie dafür, dass nicht mehr benötigte Datenträger vollständig vernichtet werden. Vergewissern Sie sich, dass keine Papiere allgemein zugänglich zurückbleiben.
- Arbeiten Sie mit Ihren Ansprechpartnern beim Kunden zusammen: Das schafft Vertrauen und entlastet Sie selbst.

1.8 Feedback

Um diese Systembeschreibung ständig verbessern und korrigieren zu können, benötigen wir Ihre Hilfe. Insbesondere interessiert uns Ihre Meinung zu den folgenden Punkten:

- Wo fehlen Einzelheiten? Wo ist die Beschreibung zu detailliert?
- Wo sollten mehr Grafiken zur Veranschaulichung verwendet werden?
- An welchen Stellen ist die Beschreibung schwer verständlich?
- Welche Punkte sollten noch in diese Beschreibung aufgenommen werden?

Bitte senden Sie Ihre Anmerkungen an:

Siemens Enterprise Communications GmbH & Co. KG
Fachredaktion
SEN ESY SME HW 42
Hofmannstr. 51
D-81359 München
Fax.: + 49 89 722 32474

Damit wir Ihnen gegebenenfalls antworten oder mit Ihnen Kontakt aufnehmen können, geben Sie bitte auch Ihre Adresse und Telefon- oder Fax-Nummer an.

1.9 Copyright

2 Systemübersicht HiPath 2000

HiPath 2000 bietet die Vorteile und Flexibilität der IP-Technologie, z. B. für die einfache Anbindung von Filialen und Teleworkern. Hoher Sprachkomfort und Zuverlässigkeit der traditionellen Telephonie bleiben natürlich erhalten.

- Voller ComScendeo-Leistungsumfang in der IP-Infrastruktur mit integrierter Router-Funktion und 4-Port-LAN-Switch
- Niedrige Anschaffungskosten
- Flexible Erweiterung über User-Lizenzen
- Wirtschaftliche Integration in HiPath-Netze über CorNet-IP
- Gesicherte IP-Kommunikation durch IPSec und VPN
- Einfache Administration über Web-based Management
- Nutzung von Internet-Telefonie Service Provider (ITSP) Services

2.1 Leistungsmerkmalbeschreibung

HiPath 2000 V1.0 ist die Produktfamilie für die rein IP-basierte Kommunikation.

HiPath 2000 nutzt das Betriebssystem LINUX (Unter Linux wird heute allgemein ein freies und portables Betriebssystem für Computer verstanden).

HiPath 2000 stellt auf IP-Basis alle TDM-Leistungsmerkmale bereit.

Die detaillierte Beschreibung aller Leistungsmerkmale können Sie der Leistungsmerkmalbeschreibung HiPath 2000 V1.0 entnehmen.

2.2 Hardware

2.2.1 Hardware-Systemarchitektur

HiPath 2020 und HiPath 2030 sind die neuen Modelle der HiPath 2000-Systemfamilie.

Einsatzgebiet sind Standalone-Kunden und die Integration in HiPath 3000 (ab V5.0)- / HiPath 5000 (ab V5.0)-Netze. HiPath 2000 ist zusammen mit HiPath 33x0/35x0/37x0/3800-Modellen im vollen Cornet-IP-Leistungsumfang lauffähig.

Ebenso möglich ist der Einsatz in HiPath 4000 (ab V2.0)-Netzen über Cornet-IP.

Beide Modelle werden mit festem HW-Ausbau geliefert (nicht erweiterbar) und eignen sich sowohl für die Wandinstallation, die Tischaufstellung oder für den Einbau in Standard-19”-Schränke (ohne Zusatzkühlung). Bis zu 4 IP-Workpoints können direkt an die HiPath 2000 angeschlossen werden.

Zusätzliche IP-Workpoints werden über ComScendo-Lizenzen freigeschaltet (siehe Abschnitt 1.4, “Lizenzierung”).



2.3 Systemfamilien und dazugehörige Modelle

Die Systeme der HiPath 2000 decken durch die individuellen Gehäusekonstruktionen und die variablen Anschlussmöglichkeiten ein breites Kundenspektrum ab.

Varianten

Die Systeme werden in folgenden Varianten vermarktet:

- HiPath 2020, Branch S_0
- HiPath 2020, Branch T1 (nur für USA)
- HiPath 2030, Standalone S_0
- HiPath 2030, Standalone T1 (nur für USA)

Diese unterscheiden sich unter anderem in der Ausbaustufe des Hauptplatine und durch unterschiedliche Frontblenden.

Informationen zu den Ausbaugrenzen der verschiedenen HiPath 2000-Systeme können der Tabelle 2-1 entnommen werden.

2.3.1 HiPath 2020

2.3.1.1 Hardware-Übersicht

HiPath 2020 unterstützt den Anschluss von maximal 20 IP-Workpoints und wird vorrangig als kleine Filiallösung (Branch) für HiPath 3000, HiPath 4000 und HiPath 5000 eingesetzt. Zusätzlich bestehen Anschlussmöglichkeiten für ISDN-Endgeräte (nur HiPath 2020-Variante S_0).

Die Versorgung des Systems erfolgt über eine integrierte Stromversorgung.

Gesamtansicht

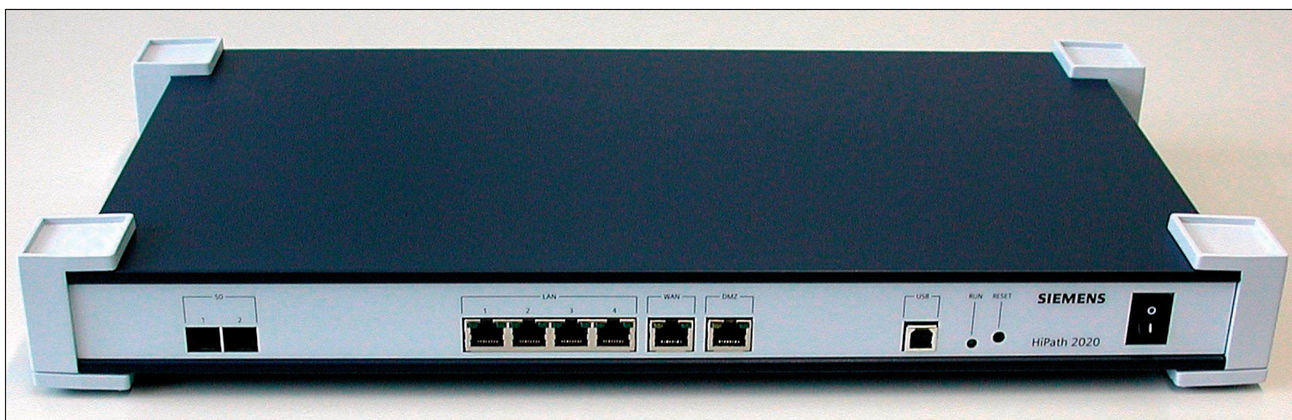


Bild 2-1 HiPath 2020 (Variante S_0) nicht für USA



Bild 2-2 Nur für USA: HiPath 2020 (Variante T1)

Anschlussmöglichkeiten

- S_0-Anschlüsse (HiPath 2020-Variante S_0, für alle Länder außer USA):
  – 2 x S_0 für den ISDN-Basisanschluss oder den ISDN-Teilnehmeranschluss
- T1-Anschluss (HiPath 2020-Variante T1, nur für USA):
  – 1 x T1 für den ISDN-Primärmultiplexanschluss (Primary Rate Interface PRI)
- LAN-Anschlüsse:
  – 4 x LAN für den direkten Anschluss von IP-Workpoints oder die weitere Verzweigung in die LAN-Infrastruktur des Kunden
  – 1 x WAN für den Anschluss an das öffentliche Netz (Provider)
  Der Anschluss der HiPath 2000 an einen Internet Telephony Service Provider (ITSP) und damit die Nutzung der DSL-Telefonie kann über einen DSL-Telefonie-Teilnehmeranschluss (ab V1.0 SMR-06) oder einen DSL-Telefonie-Anlagenanschluss mit Durchwahl (ab V1.0 SMR-09) erfolgen.
  Für die Nutzung der WAN-Schnittstelle muss HiPath 2000 direkt mit dem Internet verbunden werden. In diesem Fall muss die HiPath 2000 als Router fungieren.
  – 1 x DMZ (demilitarisierte Zone) zum Beispiel für den “DMZ-ähnlichen” Betrieb oder den Anschluss eines WLAN Standalone Access Points
- USB-Anschluss:
  1 x USB (USB V1.1, Slave Mode)

Betriebsarten

HiPath 2020 eignet sich für folgende Betriebsarten:

- Freistehend
- Wandmontiert
- Integriert im 19“-Schrank

Service

Funktionen für die Standardadministration und -wartung sind im System integriert und können über das Web-based Management WBM vorgenommen werden.

HiPath 3000 Manager E steht als Expertentool für den Servicetechniker zur Verfügung und umfasst alle Funktionen für die Inbetriebnahme, Wartung und Diagnose.

Lizenzierung

System und IP-Workpoints werden über Lizenzen freigeschaltet. Die Übernahme der Lizenzen durch das System kann über WBM oder einen IP-Workpoint erfolgen.

2.3.2 HiPath 2030

2.3.2.1 Hardware-Übersicht

HiPath 2030 unterstützt den Anschluss von maximal 30 IP-Workpoints und wird vorrangig als selbstständiges IP-Kommunikationssystem (Standalone) eingesetzt. Zusätzlich bestehen Anschlussmöglichkeiten für analoge Endgeräte und ISDN-Endgeräte (nur HiPath 2030-Variante S_0).

Darüber hinaus ist HiPath 2030 standardmäßig mit der integrierten Voice Mail ausgestattet.

Die Versorgung des Systems erfolgt über eine integrierte Stromversorgung.

Gesamtansicht

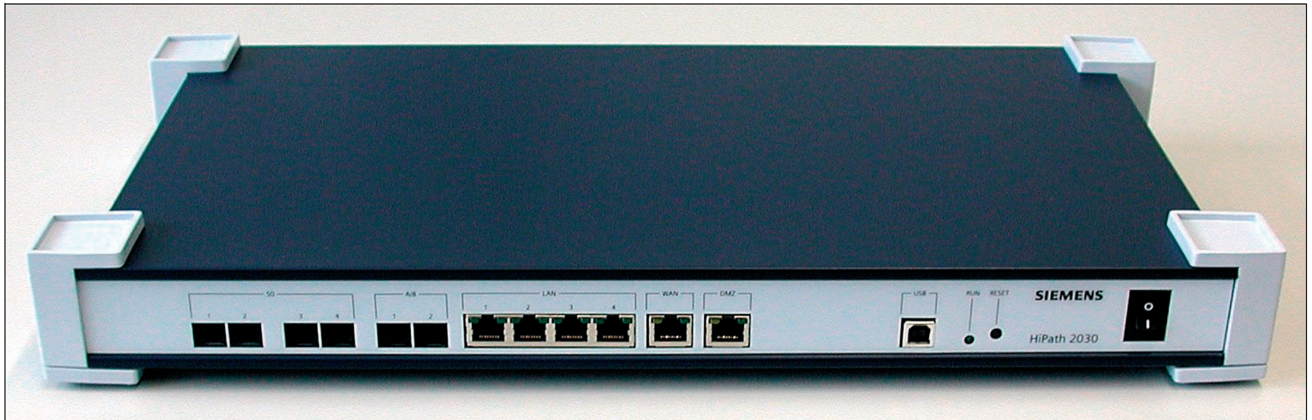


Bild 2-3 HiPath 2030 (Variante S_0) nicht für USA



Bild 2-4 Nur für USA: HiPath 2030 (Variante T1)

Anschlussmöglichkeiten

- S_0-Anschlüsse (HiPath 2030-Variante S_0, für alle Länder außer USA):
  - 4 x S_0 für den ISDN-Basisanschluss oder den ISDN-Teilnehmeranschluss
- T1-Anschluss (HiPath 2030-Variante T1, nur für USA):
  - 1 x T1 für den ISDN-Primärmultiplexanschluss (Primary Rate Interface PRI)
- Analoge Anschlüsse:

  2 x a/b (RJ45-Buchsen) für den Anschluss von analogen Endgeräten z.B. Fax-Gruppe 3
- LAN-Anschlüsse:
  - 4 x LAN für den direkten Anschluss von IP-Workpoints oder die weitere Verzweigung in die LAN-Infrastruktur des Kunden
  - 1 x WAN für den Anschluss an das öffentliche Netz (Provider)
    Der Anschluss der HiPath 2000 an einen Internet Telephony Service Provider (ITSP) und damit die Nutzung der DSL-Telefonie kann über einen DSL-Telefonie-Teilnehmeranschluss (ab V1.0 SMR-06) oder einen DSL-Telefonie-Anlagenanschluss mit Durchwahl (ab V1.0 SMR-09) erfolgen.
    Für die Nutzung der WAN-Schnittstelle muss HiPath 2000 direkt mit dem Internet verbunden werden. In diesem Fall muss die HiPath 2000 als Router fungieren.
  - 1 x DMZ (demilitarisierte Zone) zum Beispiel für den “DMZ-ähnlichen” Betrieb oder den Anschluss eines WLAN Standalone Access Points
- USB-Anschluss:

  1 x USB (USB V1.1, Slave Mode)

Betriebsarten

HiPath 2030 eignet sich für folgende Betriebsarten:

- Freistehend
- Wandmontiert
- Integriert im 19“-Schrank

Service

Funktionen für die Standardadministration und -wartung sind im System integriert und können über das Web-based Management WBM vorgenommen werden.

HiPath 3000 Manager E steht als Expertentool für den Servicetechniker zur Verfügung und umfasst alle Funktionen für die Inbetriebnahme, Wartung und Diagnose.

Lizenzierung

System und IP-Workpoints werden über Lizenzen freigeschaltet. Die Übernahme der Lizenzen durch das System kann über WBM oder einen IP-Workpoint erfolgen.

2.4 Systembedingte Ausbaugrenzen

Die Berechnung der maximalen Ausbaugrenzen basiert auf einer durchschnittlichen Verkehrsleistung von 0,15 Erlang.

Aus vertrieblichen Gründen können abweichende Ausbaugrenzen festgelegt werden.

System		HiPath 2020		HiPath 2030	
		Variante S_0	Variante T1	Variante S_0	Variante T1
Teilnehmer:					
	Summe TDM- + IP-Teilnehmer	22[1]	20	36[1]	32
	IP-Teilnehmer (System Clients, H.323 Clients, SIP Clients, WLAN-Teilnehmer)	20		30	
	Summe TDM-Teilnehmer	2[1]	–	6[1]	2
	Analoge Teilnehmer	–		2	
	ISDN-Teilnehmer	2[1]	–	4[1]	–
Leitungen:					
	Summe der B-Kanäle digitaler Amtsleitungen (S_0, fractional T1)	4[1]	8	8[1]	8
	CorNet-IP-Vernetzungsleitungen	8		8	

Tabelle 2-1 HiPath 2000- Systembedingte Ausbaugrenzen (Maximalzahlen)

1 Die S_0-Schnittstellen können für den ISDN-Basisanschluss oder den ISDN-Teilnehmeranschluss genutzt werden.

2.4.1 Statische Konfigurationsregeln

2.4.1.1 Ressourcen und Ausbaugrenzen

HiPath 2000 stellt die in Tabelle 2-2 genannten Ressourcen zur Verfügung. Tabelle 2-3 zeigt die systemspezifischen Ausbaugrenzen (Maximalzahlen) für die zugehörigen Funktionen.

Ressource	HiPath 2020	HiPath 2030
Routing-Kanäle Ein Routing-Kanal ist zum Beispiel erforderlich, um eine Verbindung zwischen zwei IP-Netzen via ISDN herzustellen (ISDN Routing).	2	

Tabelle 2-2 Ressourcen

Ressource	HiPath 2020	HiPath 2030
Gateway-Kanäle (DSP-Kanäle) Ein Gateway-Kanal wird zum Beispiel für die Verbindung zwischen einem IP-Workpoint und einem TDM-Workpoint benötigt.	8 Durch die Aktivierung folgender Leistungsmerkmale wird die Anzahl der verfügbaren Gateway-Kanäle (DSP-Kanäle) reduziert: ● QoS Data Collection QDC aktiviert: 7 ● Direct Media Connection DMC aktiviert: 6 ● QDC + DMC aktiviert: 5 Pro analogem Modem-Zugang werden zwei Gateway-Kanäle (DSP-Kanäle) belegt. Beispiel: HiPath 2030 hat DMC aktiviert und verwendet einen analogen Modem-Zugang. Damit verbleiben 4 Kanäle für Voice/Fax-Verbindungen.	
Fax- / Modem-Kanäle (G.711)	8	
Fax-Kanäle (T.38) Hierbei handelt es sich um spezielle HW-Ressourcen, die Fax über IP-Funktionalität mit dem T.38-Protokoll ermöglichen.	-	
Teleworker mit AES-Verschlüsselung	10	
DMC-Kanäle Hierbei handelt es sich um die Gateway-Kanäle für Direct Media Connections DMC mit HiPath 4000 (Leistungsmerkmal DMC Interworking ist aktiviert.[1]).	6	
MOH-Kanäle (G.711, G.723, G.729) Die Anzahl der verwendeten MOH-Kanäle ist abhängig von der Konfiguration (WBM, HiPath 3000 Manager E).	0 – 5	

Tabelle 2-2 Ressourcen

1 Die Anzahl der verfügbaren Gateway-Kanäle (DSP-Kanäle) wird reduziert, sobald das Leistungsmerkmal DMC Interworking mittels WBM oder HiPath 3000 Manager E aktiviert wurde.

Tabelle 2-3 Systemspezifische Ausbaugrenzen (Maximalzahlen)

Funktion	HiPath 2020	HiPath 2030
PPP Routing Partner	70	
MOH-Datenströme	10	

2.4.1.2 Gateway-Kanäle (DSP-Kanäle)

2.4.2 Gateway-Kanäle (DSP-Kanäle)

Für Verbindungen von IP-Workpoints (System Clients, H.323 Clients, SIP Clients) zu TDM-Workpoints und -Leitungen werden Gateway-Kanäle benötigt. Dies sind zum Beispiel Verbindungen zu Amtsleitungen, analogen Teilnehmern und ISDN-Teilnehmern.

HiPath 2000 unterstützt die Anbindung an Internet Telephony Service Provider (ITSP) und damit die Nutzung der DSL-Telefonie. Auch für Verbindungen zu einem ITSP werden Gateway-Kanäle benötigt.

Bei Konferenzen werden Gateway-Kanäle entsprechend der Anzahl der beteiligten Teilnehmer und IP-Workpoints belegt.

2.4.2.1 MOH-Kanäle (G.711, G.723, G.729)

HiPath 2000 stellt eine feste MOH-Ansage zur Verfügung. Über das WBM kann eine individuelle Ansage im System eingerichtet werden.

Pro aktiviertem MOH-Codec wird ein DSP-Kanal reserviert, um MOH in der entsprechenden Codierung (G.711, G.729, ...) für IP-Workpoints bereitzustellen. Werden zum Beispiel alle fünf MOH-Codecs aktiviert (= fünf reservierte DSP-Kanäle), verbleiben nur noch drei DSP-Kanäle für Voice-Verbindungen.

Hinweis: Der für MOH aktivierte Codec muss mit einem der von den IP-Workpoints verwendeten Codecs identisch sein.

2.4.2.2 IP-Networking-Kanäle (PBX-Networking-Kanäle)

Für die Verbindung zwischen Kommunikationssystemen werden IP-Networking-Kanäle verwendet. Dabei wird unterschieden zwischen Verbindungen, die einen Gateway-Kanal erfordern, und direkten Payload-Verbindungen. Abhängig von der Verbindungsart sind die folgenden Ressourcen für einen erfolgreichen Verbindungsaufbau erforderlich.

Verbindungsart	Leitung	Gateway-Kanal
direkte Payload-Verbindung	erforderlich	nicht erforderlich
Gateway-Verbindung	erforderlich	erforderlich

Steht eine der erforderlichen Ressourcen nicht zur Verfügung, wird der Verbindungswunsch abgewiesen.

Mittels WBM oder HiPath 3000 Manager E wird definiert, wieviele der maximal möglichen Leitungen als IP-Networking-Kanäle (IP-Vernetzungsleitungen) eingerichtet werden sollen. Die systembedingten Maximalzahlen der IP-Vernetzungsleitungen können Tabelle 2-3 entnommen werden.

2.4.2.3 DMC (Direct Media Connection)-Kanäle

Bei einer IP-Vernetzung zwischen HiPath 2000 und HiPath 4000 mit aktiviertem Leistungsmerkmal DMC-Interworking werden Gateway-Verbindungen über sogenannte DMC-Kanäle realisiert. Aus Anwendersicht ist ein DMC-Kanal ein Gateway-Kanal, der eine Gateway-Verbindung zwischen HiPath 2000 und HiPath 4000 bereitstellt. Da ein DMC-Kanal sowohl eine Master- als auch eine Slave-Verbindung bedienen muss, kommt es zu einer Reduzierung der DSP-Kanäle.

Hinweis: Die Anzahl der verfügbaren Gateway-Kanäle (DSP-Kanäle) wird reduziert, sobald das Leistungsmerkmal DMC-Interworking mittels WBM oder HiPath 3000 Manager E aktiviert wurde. In diesem Fall kann ein Digital Signal Processor DSP nur 80 % seiner maximal möglichen Kanäle bereitstellen (zum Beispiel 6 anstatt 8 DSP-Kanäle).

2.4.2.4 ISDN-Routing / PPP-Kanäle

HiPath 2000 kann auch als ISDN-Router genutzt werden. Der ISDN-Router hat die Funktion, zwei räumlich getrennte IP-Netzwerke über eine ISDN-Leitung miteinander zu verbinden. Durch Kanalbündelung kann die erforderliche Bandbreite angepasst werden.

Das System reserviert die für ISDN-Routing erforderlichen B-Kanäle und schränkt damit die vorhandenen Gateway-Kanäle ein.

Tabelle 2-4 Systemspezifische Summe der PPP-Kanäle und Gateway-Kanäle (

	HiPath 2020	**HiPath 2030**
PPP-Kanäle (Routing-Kanäle)	maximal 2	
Gateway-Kanäle (DSP-Kanäle)	maximal 8	
Summe der PPP-Kanäle **und** Gateway-Kanäle	maximal 8	

2.4.2.5 Fax- / Modem-Kanäle

Fax- und Modem-Übertragungen können sowohl über transparente G.711-Gateway-Kanäle als auch über T.38-Kanäle (nur Fax) erfolgen.

T.38 bietet zwar die zuverlässigere Fax-Übertragungsmethode, kann aber nur bis maximal 14 kBit/s genutzt werden. Durch die für T.38 erforderliche höhere Prozessorleistung ist die Anzahl der verfügbaren T.38-Kanäle begrenzt. Alternativ können G.711-Gateway-Kanäle für Fax-Übertragungen verwendet werden.

Fax-Übertragungen bei DSL-Telefonie sind ausschließlich über G.711-Gateway-Kanäle möglich.

Modem-Übertragungen sind aufgrund technischer Einschränkungen bei DSL-Telefonie nicht möglich.

Hinweis: Die Anzahl der verfügbaren G.711-Gateway-Kanäle wird reduziert, sobald das Leistungsmerkmal DMC-Interworking aktiviert wurde.

2.5 Technische Daten

Systemwerte	HiPath 2020	HiPath 2030
Anschlusswerte (Typenschild)	110 – 240 VAC 1,0 A	110 – 240 VAC 1,0 A
Netzfrequenz	50 – 60 Hz	50 – 60 Hz
Abmessungen (Höhe x Breite x Tiefe in mm)	44 x 440 x 240 (55 x 478 x 240 einschließlich Gehäusefüße)	44 x 440 x 240 (55 x 478 x 240 einschließlich Gehäusefüße)
Höheneinheiten für 19”-Schrank-montage	1	1
Gewicht	ca. 3,0 kg	ca. 3,0 kg

Tabelle 2-5 Technische Daten

2.6 Schnittstellenreichweiten

Endgeräte-Schnittstellenreichweiten für HiPath 2030

Endgeräte-Schnittstellen	Reichweite in m	Schleifenwiderstand in Ohm
ISDN-S_0-erweiterte Bus-Verbindung	< 400	104
ISDN-S_0-Bus-Verbindung	< 120	21
ISDN-S_0-Anschlussdose zum Endgerät	< 10	–
a/b-Teilnehmer	< 2000	520

Tabelle 2-6 Endgeräte-Schnittstellenreichweiten für HiPath 2030 (bei J-Y (ST) 2x2x0,6, 0,6 mm Durchmesser)

Amtsanschluss-Reichweiten

Die folgende Tabelle nennt max. mögliche Leitungslängen für den Amtsanschluss. Die Werte gelten für ideale Bedingungen, das heißt es dürfen keine Stoßstellen etc. vorhanden sein. Die realen Verhältnisse sind nur messtechnisch an Ort und Stelle erfassbar.

Schnittstelle	Kabel	Durchmesser	Dämpfung pro km	max. Leitungslänge
S_0	ICCS-Kabel J-2Y(ST)Y4x2x0,51 LG ICCS Data5	0,51 mm	7,5 dB bei 96 kHz	800 m
	Installationskabel J-2Y(ST)Y ≥ 10x2x0,6 ST III BD	0,6 mm	6,0 dB bei 96 kHz	1000 m

Tabelle 2-7 Leitungslängen für den Amtsanschluss

2.6.1 Geplante Sprachen

Zum Vertriebsstart werden die Sprachen Deutsch und Englisch freigegeben. Die weiteren Sprachen werden im Zuge der Ländereinführungen bereitgestellt:

Sprache	Systemmeldungen	Integrierte Voice Mail	HiPath 2000 Manager (WBM)	HiPath Manager E
Deutsch	●	●	●	●
Englisch (US)	●	●	●	●
Englisch (UK)	●	●	●	●
Bulgarisch	●			

Sprache	Systemmeldungen	Integrierte Voice Mail	HiPath 2000 Manager (WBM)	HiPath Manager E
Dänisch	●			●
Finnisch	●			●
Flämisch		●		
Französisch	●	●	●	●
Französisch (Kanada)		●		
Griechisch	●	●		●
Italienisch	●	●	●	●
Lettisch	●			
Litauisch	●			
Niederländisch	●	●	●	●
Norwegisch	●			
Polnisch	●			●
Portugiesisch	●	●	●	●
Portugiesisch (Brasilien)		●		
Rumänisch	●			
Russisch	●			●
Schwedisch	●			●
Slowakisch	●			
Slowenisch	●			
Spanisch	●	●	●	●
Spanisch (Lateinamerika)		●		
Tschechisch	●	●		
Türkisch	●	●		
Ungarisch	●			●

- **Systemmeldungen**: Meldungen z.B. in den Displays der Telefone.
- **Integrierte Voicemail**: ausschließlich HiPath 2030
- **Web-based Manager**: integriert in HiPath 2020 und HiPath 2030
- **HiPath Manager E**: Administrations-Software der HiPath 2000/3000/5000 für den Service

2.7 Technische Vorschriften und Konformität

2.7.1 CE-Konformität (nicht für USA)

Basis der CE-Kennzeichnung ist die R&TTE-Directive 99/5/EEC.

	Normenreferenz
Safety	EN 60950:2000
EMC Emission	EN 55022:1998 Class A (EMC, Emission ITE Residential Environment) EN 55024:1998 (EMC, Immunity ITE Residential Environment) EN 61000-3-2:2000 Class A (EMC, Harmonic Current Emissions)
EMC Immunity	EN 50371:2002 (EMF, General Public Human Field Exposure)

2.7.2 Konformität mit US- und kanadischen Normen (nur für USA und Kanada)

	Normenreferenz
Safety	UL 60950-1
EMC Emission	FCC Part 15 Subpart B Class A
Transmission USA	FCC Part 68
Transmission Kanada	CS-03

2.7.2.1 Konformität mit FCC und Industry Canada

Im folgenden werden die Anforderungen für die Konformität mit der Federal Communications Commission (FCC) sowie dem kanadischen Industriestandard CS-03 beschrieben.

2.7.2.2 FCC-Registrierung und Anforderungen

In den nachfolgenden Abschnitten werden die Anforderungen und Inhalte der FCC-Richtlinien beschrieben.

2.7.2.2.1 Service

Bei Problemen mit Produkten der HiPath 2000-Modellreihe sollten Sie sich mit dem Siemens Enterprise Communications GmbH & Co. KG-Kundendienst (1-800-TEL-ROLM) in Verbindung setzen; Sie erhalten hier weitere Informationen zu Service- und Reparaturleistungen. Die Telefongesellschaft bittet Sie möglicherweise, die angeschlossenen Geräte bis zur Behebung des Problems vom Netz zu nehmen bzw. bis sichergestellt ist, dass keine Gerätestörung vorliegt.

2.7.2.2.2 FCC-Vorschriften, Teil 15

Die HiPath 2000-Systeme wurden getestet und liegen innerhalb der Grenzwerte für Digitalgeräte der Klasse A gemäß Teil 15 der FCC-Richtlinien. Diese Grenzwerte wurden so festgelegt, dass ein angemessener Schutz gegen Funkstörungen in einer gewerblichen Umgebung gewährleistet ist. Von diesen Geräten wird Hochfrequenzenergie erzeugt, genutzt und eventuell ausgestrahlt. Bei unsachgemäßer Installation und Handhabung kann es daher zu Störungen des Funkverkehrs kommen. Werden solche Geräte in Wohngebieten eingesetzt, gehen alle erforderlichen Maßnahmen zur Beseitigung derartiger Störungen allein zu Lasten des Anwenders.

2.7.2.2.3 FCC-Vorschriften, Teil 68

FCC-Vorschriften, Teil 68 - Registrierung

Die HiPath 2000-Systeme erfüllen die Anforderungen von Teil 68 der FCC-Vorschriften. Auf der Geräteabdeckung ist ein Aufkleber angebracht, der unter anderem die FCC-Registrierungsnummer ausweist. Geben Sie diese Informationen auf Anforderung an die Telefongesellschaft weiter.

REN

Der Anschlusswert (Ringer Equivalence Number, REN) bestimmt die Anzahl der Geräte, die an die Fernsprechleitung angeschlossen werden können. Überschüssige RENs auf der Fernsprechleitung können zur Folge haben, dass die Geräte bei kommenden Anrufen kein Rufsignal ausgeben. In den meisten, jedoch nicht in allen Bereichen, sollten maximal fünf (5) RENs verfügbar sein. Um festzustellen, wie viele Geräte an eine Leitung angeschlossen werden können (d. h., wie viele RENs verfügbar sind), müssen Sie sich gegebenenfalls mit Ihrer lokalen Telefongesellschaft in Verbindung setzen.

Hinweis: RENs kommen bei analogen Leitungsschnittstellen und analogen Telefonen zur Anwendung. Für die IP-basierten HiPath 2000-Systeme werden sie nicht angewendet.

Informationen zu den Einrichtungsschnittstellen

Um eine registrierte Endeinrichtung an die Leitungen der Telefongesellschaft anschließen zu können, müssen diese Einrichtungen über FCC-seitig registrierte Anschlüsse verfügen. Die hier beschriebenen Geräte sind mit Standardsteckern ausgestattet.

Die nachfolgenden Tabellen bieten einen Überblick über die Schnittstellen der Einrichtungen, die Belegung der Netzwerkschnittstellen, die RENs oder Servicecodes sowie die Netzwerkanschlüsse.

Diese Tabelle bietet einen Überblick über die Teilnehmerschnittstellen für analoge Privatleitungsdienste (PL Services).

Hersteller-Port-ID	Facility Interface Code FIC	Service Order Code SOC	Netzanschluss
a/b (ONS)	OL13B	9.0F	RJ21C

Diese Tabelle bietet einen Überblick über die digitalen Leitungsschnittstellen für Digitaldienste.

Hersteller-Port-ID	Digital Interface Code	Service Order Code SOC	Netzanschluss
T1	04DU9-BN	6.0P	entfällt[1]
T1	04DU9-DN	6.0P	entfällt[1]
T1	04DU9-1KN	6.0P	entfällt[1]
T1	04DU9-1SN	6.0P	entfällt[1]

1 Die DIU2U-Schnittstellen sind über FCC-seitig registrierte Endeinrichtungen (Network Communications Terminated Equipment, NCTE) mit dem öffentlichen Fernsprechnetz (Public Switched Telephone Network, PSTN) verbunden. Die NCTEs definieren hierbei den zu verwendenden Netzanschlusstyp.

Diese Tabelle bietet einen Überblick über die Answer Supervision Codes für DID-Schnittstellen.

Hersteller-Port-ID	Facility Interface Code FIC	Answer Supervision Code	Netzanschluss
T1	04DU9-BN	AS.2	entfällt[1]
T1	04DU9-DN	AS.2	entfällt[1]
T1	04DU9-1KN	AS.2	entfällt[1]
T1	04DU9-1SN	AS.2	entfällt[1]

1 Die DIU2U-Schnittstellen sind über FCC-seitig registrierte Endeinrichtungen (Network Communications Terminated Equipment, NCTE) mit dem öffentlichen Fernsprechnetz (Public Switched Telephone Network, PSTN) verbunden. Die NCTEs definieren hierbei den zu verwendenden Netzanschlusstyp.

Netzstörungen

Falls ein HiPath 2000-System den Betrieb des Fernsprechnetzes stört, kann die Telefongesellschaft den Zugang vorübergehend sperren. Die Telefongesellschaft wird Sie in diesem Fall normalerweise vorab informieren. Falls dies nicht möglich ist, erfolgt die Rückmeldung zum frühestmöglichen Termin. In diesem Zusammenhang werden Sie gleichzeitig darüber informiert, dass Sie eine Beschwerde bei der FCC einreichen können.

Modifikation der Telekommunikationseinrichtungen

Die Telefongesellschaft ist befugt, die eigenen Einrichtungen, Geräte, Betriebsabläufe und Prozesse bei Bedarf anzupassen; derartige Modifikationen können gegebenenfalls den Betrieb Ihrer Geräte beeinträchtigen. In diesem Fall werden Sie jedoch normalerweise vorab benachrichtigt, damit Sie die Möglichkeit haben, Unterbrechungen des Fernsprechbetriebs zu vermeiden.

Geräte für die Sprachwiedergabe

Geräte für die Sprachwiedergabe wie Wartemusik- und Sprachaufzeichnungsgeräte müssen von Siemens Enterprise Communications GmbH & Co. KG genehmigt und gemäß den Richtlinien und Bestimmungen von Absatz C der FCC-Vorschriften, Teil 68, registriert sein bzw. über geeignete Schutzschaltungen angeschlossen werden, die ebenfalls von Siemens Enterprise Communications GmbH & Co. KG zu genehmigen sind und gemäß den Richtlinien und Bestimmungen von Absatz C der FCC-Vorschriften, Teil 68, registriert werden müssen.

Neue Ortsnetz- und Amtskennzahlen

Die Leistungsmerkmale der Routing-Software für den Benutzerzugang zum Netz müssen entsprechend aktualisiert werden, damit neu eingerichtete Ortsnetzkennzahlen und Amtskennzahlen bei Implementierung erkannt werden.

Erfolgt keine Aktualisierung der installierten Systeme oder Peripheriegeräte für die Erkennung der neuen Kennzahlen, können die Kunden bzw. die Mitarbeiter am Kundenstandort keine Netzzugriffe durchführen und die neuen Kennzahlen nicht nutzen.

Geräte mit Durchwahl (Direct Inward Dialing, DID)

Werden Geräte in einer Art und Weise betrieben, die eine ordnungsgemäße Überwachung der Rufannahme verhindert, so stellt dies eine Verletzung der Bestimmungen von Teil 68 der FCC-Vorschriften dar.

Eine ordnungsgemäße Überwachung der Rufannahme ist in folgenden Fällen gewährleistet:

a) Die Geräte unterstützen eine Rückmeldung an das PSTN, wenn Durchwahlverbindungen:

- von dem gerufenen Teilnehmer entgegengenommen werden.

- von der Vermittlungsperson entgegengenommen werden.
- an eine vom CPE-Benutzer verwaltete gespeicherte Ansage weitergeleitet werden.
- an eine Wahlaufforderung weitergeleitet werden.

b) Die hier beschriebenen Geräte unterstützen eine Rückmeldung an das PSTN für alle Durchwahlverbindungen, die an das PSTN weitergeleitet werden. Zulässige Ausnahmen:

- Ein Anruf wird nicht entgegengenommen.
- Ein Besetztton (Busy Tone) ertönt.
- Ein Besetztton (Reorder Tone) ertönt.

Eignung für Hörgeschädigte

Notruftelefone sowie Telefone in frei zugänglichen Bereichen wie Eingangshallen, Krankenhauszimmern, Aufzügen und Hotelzimmern müssen mit Handapparaten ausgestattet sein, die den Einsatz magnetisch gekoppelter Hörhilfen ermöglichen. Für hörgeschädigte Personen, die sich nicht in öffentlichen Bereichen aufhalten, müssen bei Bedarf ebenfalls geeignete Handapparate bereitgestellt werden.

Die digitalen Telefone für die Siemens Enterprise Communications GmbH & Co. KG HiPath 2000-Systeme sind für den Einsatz durch Hörgeschädigte geeignet und erfüllen die Anforderungen der Abschnitte 68.316 und 68.317 von Teil 68 der FCC-Vorschriften.

Programmierbare Wählfunktionen

Wenn Sie Notrufnummern programmieren oder über ein Produkt der Siemens Enterprise Communications GmbH & Co. KG mit programmierbaren Wählfunktionen eine Testverbindung zu einer Notrufnummer herstellen, müssen Sie die Verbindung halten und dem Einsatzleiter kurz den Grund Ihres Anrufs erklären, bevor Sie auflegen. Diese Maßnahmen sollten zu verkehrsarmen Zeiten erfolgen, beispielsweise früh morgens oder spät abends.

Anschluss externer Teilnehmereinrichtungen

Externe Teilnehmereinrichtungen (Off-Premise Stations, OPS) werden von HiPath 2000-Systemen nicht unterstützt.

Voraussetzungen für den gleichberechtigten Zugriff

So genannte "Call Aggregators" (Hotels, Krankenhäuser, Flughäfen etc.) müssen die erforderlichen gleichberechtigten Endbenutzer-Zugangscodes für die vom Benutzer gewünschten Netzbetreiber (Internet Service Provider (ISP)) bereitstellen. Die aktuellen Zugangscodes lauten 10XXX, 800, 888 oder 950.

Über gleichberechtigte Zugangscodes unterstützen die HiPath 2000-Systeme den Benutzerzugang zu landesübergreifenden Anbietern (Interstate Provider) von Vermittlungsdiensten. Modifikationen dieser Funktionalität stellen eine Verletzung des Telephone Operator Consumer Services Improvement Act von 1990 sowie Teil 68 der FCC-Vorschriften dar.

Empfehlungen zur elektrischen Sicherheit

Die HiPath 2000-Systeme erfüllen sämtliche Richtlinien und Bestimmungen der FCC-Vorschriften. Es wird empfohlen, den Wechselstromausgang, an dem das HiPath 2000-System angeschlossen wird, mit einem Überspannungsschutz auszustatten, der hinsichtlich Ausführung und Leistung für das jeweils angeschaffte Modell geeignet ist. Klären Sie eventuelle Fragen zum Überspannungsschutz mit Ihrem Händler.

2.7.2.3 Einschränkungen für den Geräteanschluss

Bei den nachfolgenden Hinweisen handelt es sich um Anforderungen für die "Konformitätsbescheinigung und Registrierung von Endeinrichtungen" (Procedure for Declaration of Conformity and Registration of Terminal Equipment) gemäß Industry Canada Terminal Attachment Program Procedure DC-01(E), Abschnitt 6.4.

Konformitätsbescheinigung

Die hier beschriebenen Geräte entsprechen den geltenden technischen Spezifikationen für Endeinrichtungen gemäß der Industry Canada Terminal Equipment Technical Specification.

Ringer Equivalence Number (REN)

Hinweis: Der Anschlusswert (Ringer Equivalence Number, REN) gilt nicht für dieses VoIP (Voice over Internet Protocol)-Gateway. Die einem Endgerät zugewiesene REN gibt an, wie viele Endgeräte maximal an die Telefonie-Schnittstelle angeschlossen werden können. Der Abschluss einer Schnittstelle kann eine beliebige Gerätekombination umfassen, vorausgesetzt die REN-Anzahl aller Geräte ist nicht größer als fünf.

2.7.3 Konformität mit internationalen Normen

	Normenreferenz
Safety	IEC 60950-1
EMC Emission	CISPR22 Class A EN 61000-3-2:1995 Class A EMC, Harmonic Current Emissions
EMC Immunity	CISPR24

2.8 Umweltbedingungen

2.8.1 Elektrische Betriebsbedingungen

- Grenzbetriebsbereich
  Raumtemperatur: + 5 ...+ 40 °C (41 ... 104 °F)
  absolute Luftfeuchte: 2 ... 25 g H_2O/m^3
  relative Luftfeuchte: 5 ... 80 %
- Die Entlüftung der Anlagen erfolgt durch Konvektion.



Vorsicht
Direkte Sonneneinstrahlung oder Wärmeeinwirkung durch Heizkörper auf die Anlage ist unzulässig (Gefahr lokaler Temperaturerhöhungen).
Betaute Anlagen müssen vor der Inbetriebnahme abgetrocknet sein. Die Inbetriebnahme einer betauten Anlage ist unter allen Umständen zu vermeiden.

2.8.2 Mechanische Betriebsbedingungen

Die Anlagen sind grundsätzlich für stationären Einsatz entwickelt worden.

3 Vernetzung

3.1 IP-Vernetzungsmöglichkeiten

HiPath 2000 unterstützt die IP-Vernetzung in HiPath 3000, 4000 und 5000.

3.1.1 Protokolle

HiPath-Systeme	HiPath 2000 V1.0
HiPath 2000 V1.0	CorNet IP, SIP
HiPath 3000/5000 CS V5.0	CorNet IP
HiPath 3000/5000 CS V6.0	CorNet IP, SIP
HiPath 4000 V2.0	CorNet IP
HiPath 4000 V3.0	CorNet IP, SIP

3.1.2 Hinweise zur Nummerierung

HiPath 2000 unterstützt verdeckte und offene Nummerierung:

- Verdeckte (geschlossene) Nummerierung
  setzt die Eindeutigkeit aller Teilnehmerrufnummern im Netz voraus. Jeder Teilnehmer im Netz kann einen anderen Teilnehmer durch Wählen von dessen Rufnummer rufen.
- Offene Nummerierung
  bedeutet, dass ein Teilnehmer durch eine Knotenrufnummer und seine Teilnehmerrufnummer identifiziert wird. Dadurch können Teilnehmer in unterschiedlichen Knoten die gleiche Rufnummer aufweisen.

Nachfolgende Tabelle zeigt zulässige IP-Trunking-Szenarien bei der Vernetzung von HiPath 2000/3000/5000 ab V5.0 bzw. HiPath 4000 ab V2.0 via CorNet-IP .

IP-Trunking-Szenario	Nummerierung	Nummerierungsplan	Bemerkung
Reines HiPath 2000/3000 IP-Trunking	Geschlossen	Private Numbering Plan	Zulässiges Szenario, Anwahl über Internrufnummer
Reines HiPath 2000/3000 IP-Trunking	Offen	Private Numbering Plan	Zulässiges Szenario, Anwahl über Knotenrufnummer + Internrufnummer

IP-Trunking-Szenario	Nummerierung	Nummerierungsplan	Bemerkung
1 x HiPath 2000/3000 als Gateway und 1 x HiPath 5000 CS	Geschlossen	Private Numbering Plan	Zulässiges Szenario, Anwahl über Internrufnummer
1 x HiPath 2000/3000 als Gateway und 1 x HiPath 5000 CS	Offen	Nicht relevant	HiPath 5000 CS ist nicht vom PSTN erreichbar, daher nicht zulässiges Szenario
Mehrere HiPath2000/3000 als Gateways und 1 x HiPath 5000 CS	Geschlossen	Private Numbering Plan	Zulässiges Szenario, Anwahl über Internrufnummer
Mehrere HiPath 2000/3000 als Gateways und 1 x HiPath 5000 CS	Geschlossen zwischen einem Gateway und HiPath 5000 CS, offen zu den restlichen Gateways	Private Numbering Plan	Zulässiges Szenario, Anwahl über Knotenrufnummer + Internrufnummer
HiPath 2000/3000/4000/5000	Geschlossen	Private Numbering Plan	Zulässiges Szenario, Anwahl über Internrufnummer
HiPath 2000/3000/4000/5000	Geschlossen zwischen einem Gateway und HiPath 5000 CS, offen zu den restlichen Gateways	ISDN Numbering Plan	Zulässiges Szenario, jedoch keine HiPath 5000, kein Presence Service, kein netzweiter HPCO, keine netzweite CSTA-Funktionalität, keine netzweite HiPath Xpressions Compact
HiPath 4000/3000/2000	Geschlossen		Zulässiges Szenario
HiPath 4000/3000/2000	Offen		Zulässiges Szenario

3.1.3 CorNet-IP-Leistungsmerkmale Vernetzung HiPath 2000/3000 mit HiPath 4000

HiPath 2000 V1.0 und HiPath 3000 ab V5.0 unterstützen den gleichen Leistungsumfang bei einer Vernetzung über CorNet-IP.

Folgende Leistungsmerkmale für die Vernetzung mit HiPath 4000 ab V2.0 werden unterstützt:

- Transport von unbekannten Operationen und Funktionen fremder Systeme
- Berechtigungen
- Rückruf bei frei/besetzt
- Anklopfen
- Aufschalten
- Zweitanruf
- Rufnummernanzeige (Rufer, verbundener Teilnehmer)
- Namensanzeige (Rufer, verbundener, besetzter Teilnehmer)
- Rufnummernunterdrückung bzw. Namensunterdrückung
- Anrufumleitung
- Anrufweiterleitung bei frei oder besetzt
- Gebührenübertragung
- Halten/Rückfrage/Makeln
- Übergeben vor und nach Melden
- Konferenz
- Wiederanruf
- Schnelles Weitervermitteln
- Notruf (nur USA relevant)
- Briefkastenlampe
- Abwurf
- Zentrale BLF-Signalisierung für optiClient attendant
- Unterstützung netzweiter CSTA-Leistungsmerkmale, z.B. für HPCO, HiPath 5000

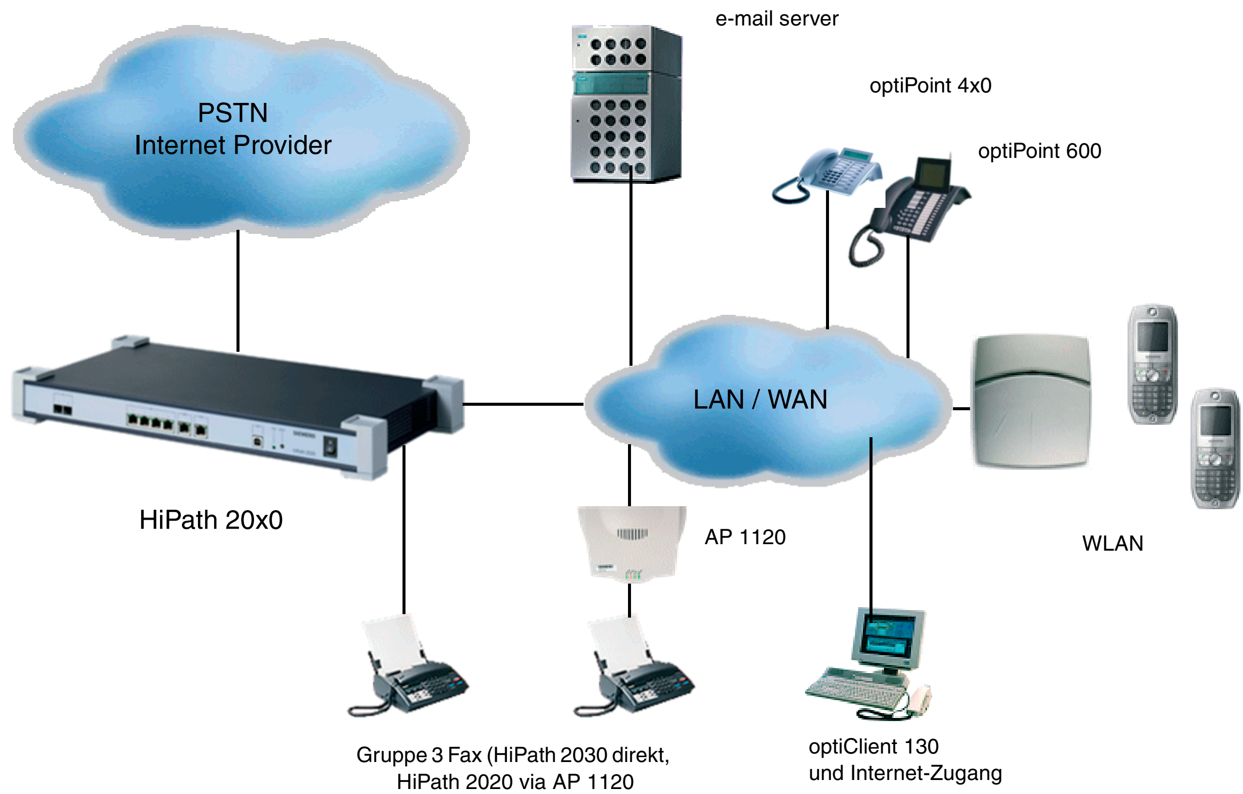
Detaillierte Beschreibungen der Vernetzungsleistungsmerkmale finden Sie in der Leistungsmerkmalbeschreibung HiPath 2000 V1.0.

3.1.4 Einsatz- und Vernetzungsszenarien über IP

Folgende Szenarien sind beschrieben:

- Einsatz als Standalone System (vorrangig HiPath 2030)
- Standalone-Szenario HiPath 2030 mit VoIP- und klassischen Endgeräten
- Anschaltung an Internet Telefonie Service Provider
- WLAN Mobilitätsszenario
- Aufbau von Virtual Private Networks (Site-to-Site-VPN-Standortvernetzung)
- Mobilitätsszenario Remote Access VPN
- Anbindung von Teleworkern über IP
- IP-Vernetzung mit mehreren HiPath 3000-Systemen und HiPath 2000
- IP-Vernetzung HiPath 2000/3000 und HiPath 5000 CS V5.0
- IP-Vernetzung: Zentrale mit HiPath 4000 und Filialen mit HiPath 2000/3000
- Small Remote Site Konzept an HiPath 4000

3.1.4.1 Einsatz als Standalone System



3.1.4.2 Standalone-Szenario HiPath 2030 mit VoIP- und klassischen Endgeräten

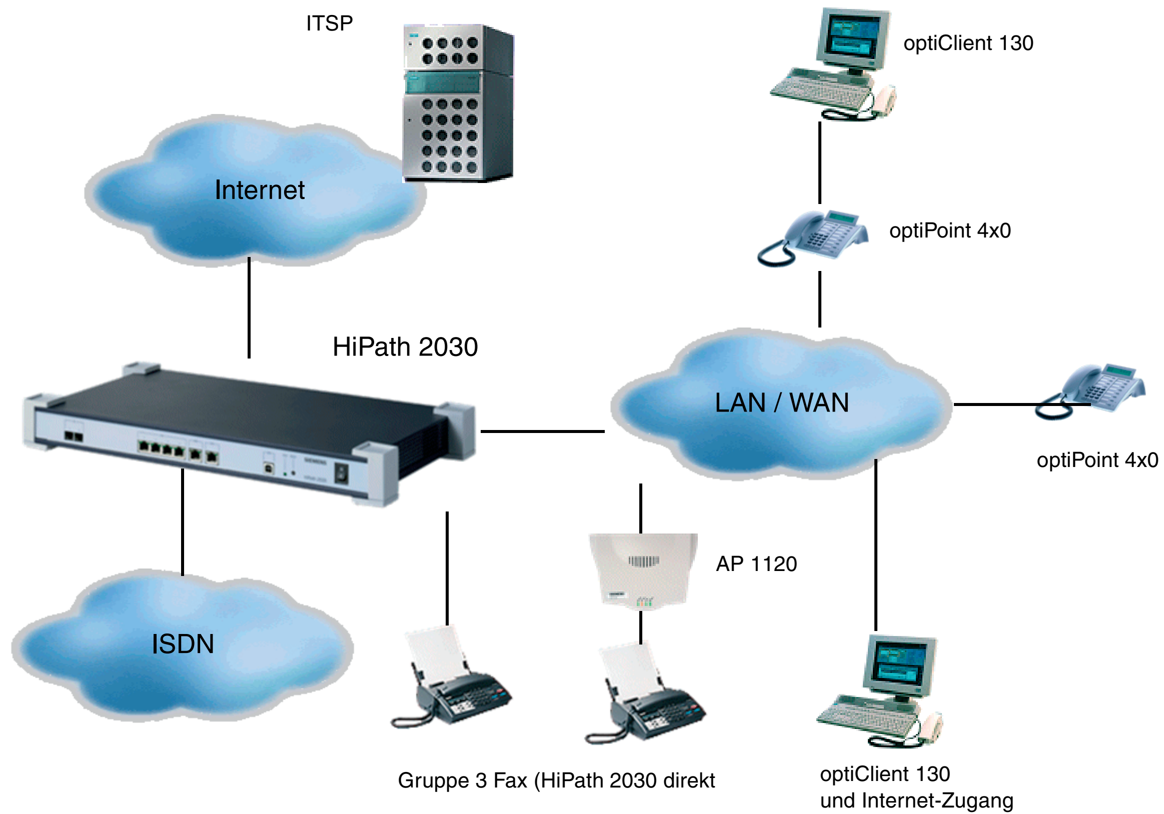
Die HiPath 2030 kombiniert IP-Router-Funktionalität mit den Telekommunikationsfunktionen eines modernen IP-Softswitch Appliance. Die IP-Workpoints der optiPoint 410/420-Familie und der optiClient 130 ermöglichen vollen ComScendo-Sprachleistungsumfang. Weiterhin können IP-Workpoints die das offene SIP-Protokoll unterstützen, angeschaltet werden. Eine Anschaltung klassischer Endgeräte wie Fax erfolgt über 2 analoge a/b-Ports oder über den Terminaladapter AP 1120. Die HiPath 2030 erlaubt ebenfalls den Anschluss von ISDN-Endgeräten an die S_0-Schnittstellen des Kommunikationssystems. Eine Vielzahl interner und externer Applikationen lassen sich nahtlos in die IT-Landschaft des Kunden integrieren. Sicherheitsfunktionen der HiPath 2000 wie Firewall und VPN-Funktionalität schaffen die Voraussetzung für gesicherte IP-Kommunikation im LAN und WAN.

Endgeräte:

- CorNet-IP-Workpoints und Clients:
  - optiPoint 410/420
  - optiClient 130
  - Standard H.323-Endgeräte: Netmeeting, Polycom SoundStation IP
- SIP-IP-Workpoints und Clients:
  - optiPoint 410 S, 420 S
  - Standard SIP-Endgeräte: MS Messenger
- Terminaladapter AP 1120

Applikationen

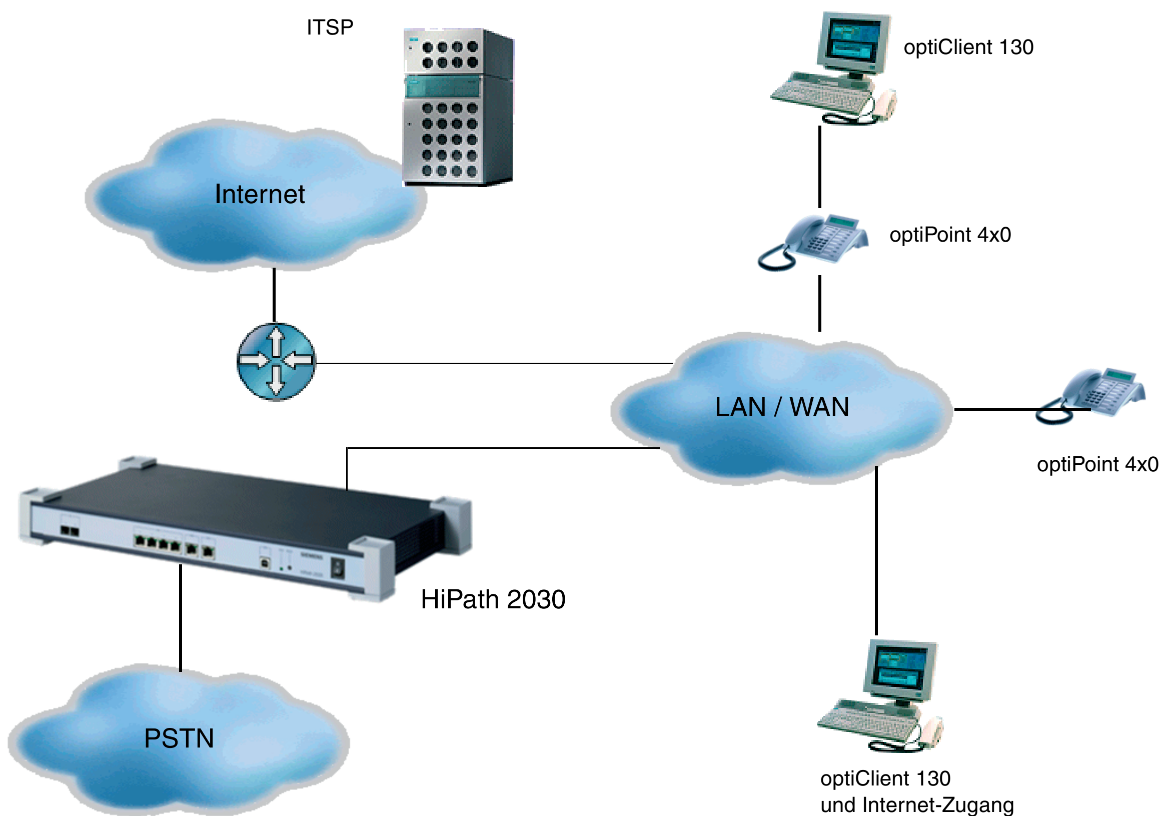
- Integrierte Voice Mail
- HiPath Mobile Office
- HiPath Meta Management


ITSP
Internet
optiClient 130
optiPoint 4x0
HiPath 2030
LAN / WAN
optiPoint 4x0
AP 1120
ISDN
Gruppe 3 Fax (HiPath 2030 direkt
optiClient 130
und Internet-Zugang

3.1.4.3 Anschaltung an Internet Telefonie Service Provider

HiPath 2000 unterstützt Anschaltungen an Internet Telefonie Service Providern (ITSP) als DSL-Telefonie-Teilnehmeranschluss mit Registrierung von Einzelrufnummern sowie für größere Systemausbauten als DSL-Telefonie-Anlagenanschluss, für den der ITSP ein Rufnummernband bereitstellt.

- Anschaltung der HiPath 2000 hinter Kunden-Router oder direkt am DSL-Modem
- NAT-Traversal mit Einsatz des STUN-Protokolls
- Optimierte Mischung von ISDN- und DSL-Leitungen
  z. B. Modem, Fax, EC Cash-Geräte über ISDN
- Bis zu 30-DSL-Telefonie-Einzelrufnummern oder Rufnummernband
- Gleichzeitige Nutzung von bis zu 4 ITSPs und ISDN Providern für die Leitweglenkung



3.1.4.4 WLAN Mobilitätsszenario

Der HiPath Wireless Access Point erleichtert kleinen Unternehmen konvergierte drahtlose Netze aufzubauen, die Sprach- und Datendienste über die selbe Infrastruktur nutzen möchten.

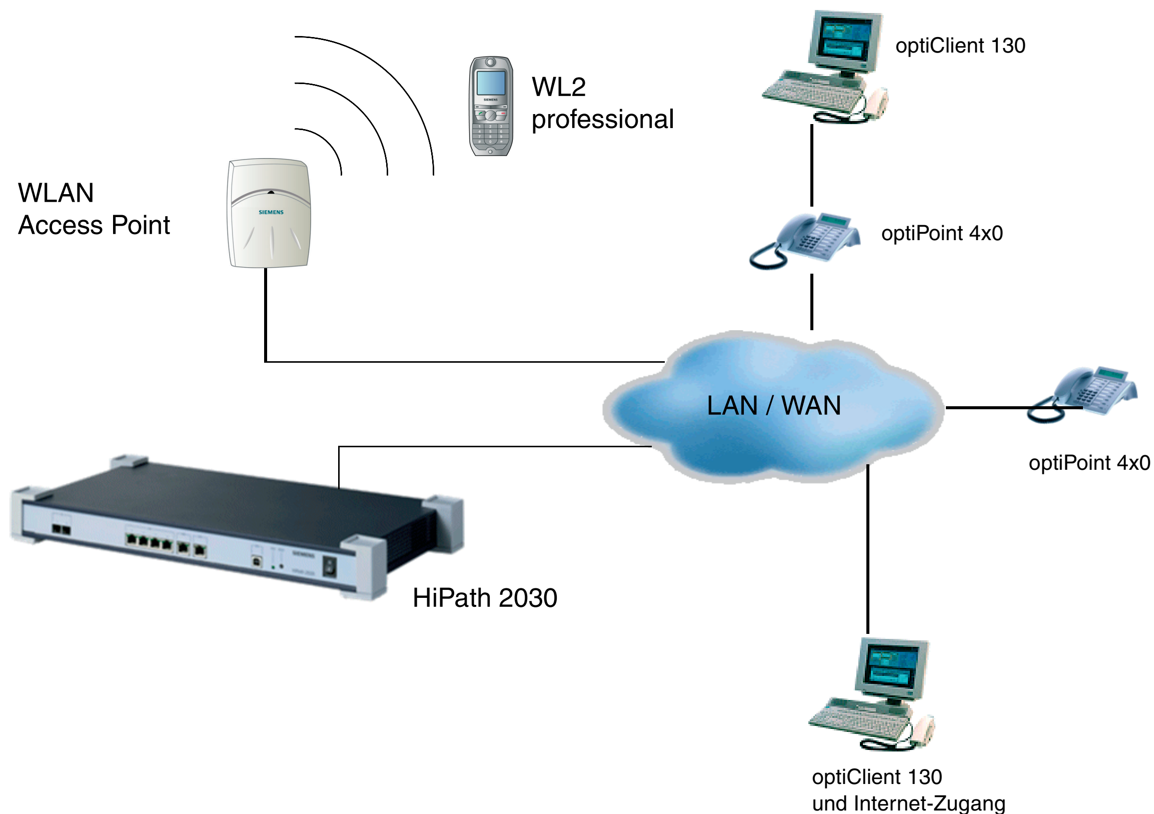
Mit optiPoint WL2 professional V1.0 (HFA) in Verbindung mit den HiPath Wireless Standalone Access Points bietet HiPath 2000 eine Komplettlösung für Daten und Voice over WLAN nach Standard 802.11 b/g.

In einem Cluster können lokal an einer HiPath 2000 bis zu 5 Access Points betrieben werden.

In Verbindung mit optiPoint WL2 professional garantieren Roaming- und Handover-Funktionen den mobilen Einsatz auf dem Firmengelände. Darüber hinaus sind Lösungen für Datenanwendungen realisierbar.

Folgende HiPath Wireless Standalone Access Points sind lieferbar:

- Wireless AP 2630 - mit interner Antenne
- Wireless AP 2640 - mit externer Antenne

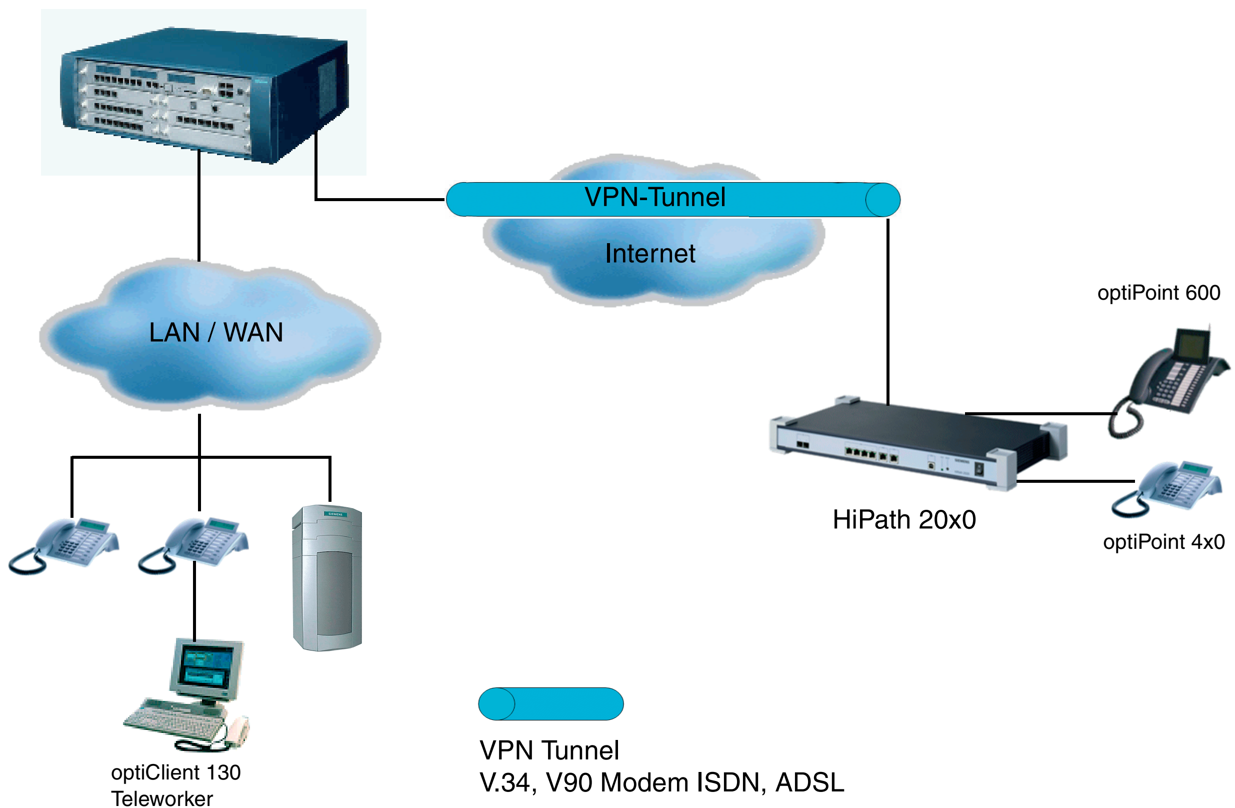


3.1.4.5 Aufbau von Virtual Private Networks (Site-to-Site-VPN-Standortvernetzung)

HiPath 2000 bietet eine sichere Lösung zur Realisierung von Site-to-Site VPNs. Die Lösung unterstützt die Vernetzung von Standorten (Hauptstandorten, Niederlassungen oder Filialen) über die kostengünstige Infrastruktur des öffentlichen Internets. Möglich sind Vernetzungen von HiPath 2000-Systemen untereinander und gemischte HiPath 2000/3000-Netze ab HiPath 3000 V5.0. Die Anbindung an das Internet kann beispielsweise über Internet-Festverbindungen oder xDSL-Anschlüsse, welche eine feste IP-Adresse bereitstellen, erfolgen. Auch Internetverbindungen mit dynamischer IP-Adresse können mittels DynDNS genutzt werden. Daten und Sprache (TDM und VoIP) werden über das Internet getunnelt. Die HiPath 2000 prüft die Authentifizierung der VPN-Partner, ver- und entschlüsselt die Datenpakete der jeweiligen Workpoints und Applikationen und stellt die Vertraulichkeit und Integrität der Daten sicher.

Vorteile der VPN Site-to-Site-Vernetzung:

- Geschützte Geschäftsprozesse
- Sichere Integration von Externen Partnern ins Firmennetz
- Zugriff auf Unternehmensinformationen für den Außendienst



3.1.4.6 Mobilitätsszenario Remote Access VPN (Anbindung von Teleworkern und mobilen Mitarbeitern)

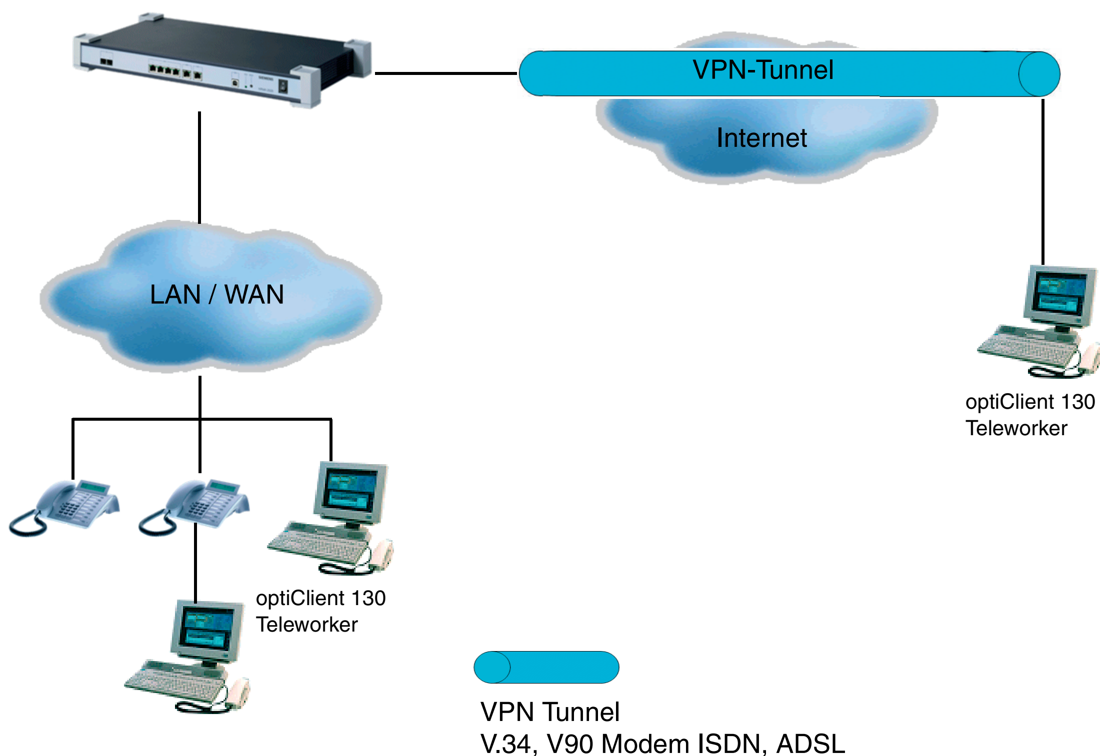
Remote Access VPN

Auch für den Fernzugriffr von mobilen Mitarbeitern, die sich über analoge, ISDN- oder ADSL-Anschlüsse in das öffentliche Internet einwählen, stellt die HiPath 2000 eine flexible Lösung bereit.

Die VPN-Client-Software Safenet Sentinel übernimmt die Authentifizierung, Ver- und Entschlüsselung auf dem PC oder Laptop des mobilen Mitarbeiters und stellt eine sichere Verbindung zur HiPath 2000 im Unternehmen her. Der VPN-Client Safenet Sentinel erhält nach erfolgreicher Anmeldung Zugriff auf das Firmen-LAN und ermöglicht Sprach- und Datenkommunikation zwischen dem mobilen Mitarbeiter und dem Unternehmen.

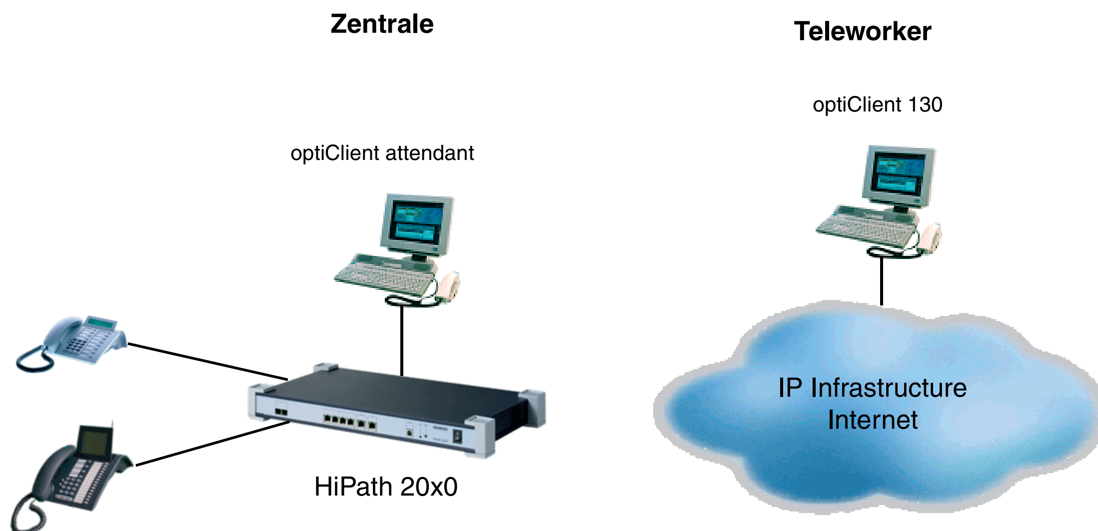
Zugriff auf zentrale Ressourcen (E-Mail, Ablagen, zentrale Anwendungen):

- Erreichbarkeit unter einer Nummer
- Einsparungspotential bei Mobilfunkgebühren
- Kostengünstige und sichere Lösung



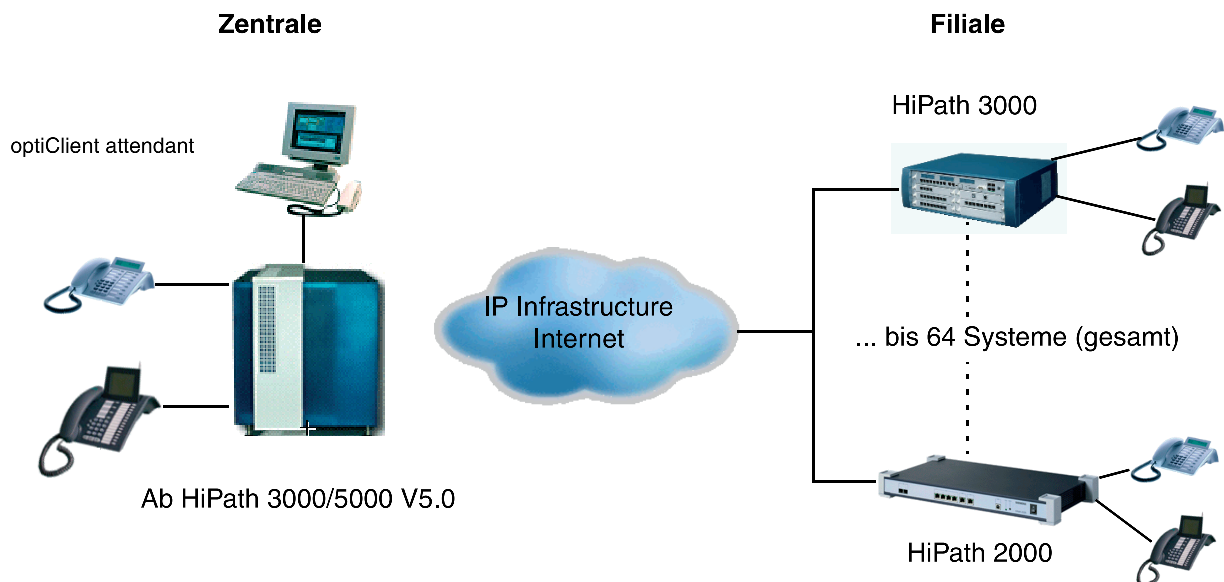
3.1.4.7 Anbindung von Teleworkern über IP

- Erreichbarkeit unter zentraler Firmennummer
- Integration in Call Center-Lösung, z.B. für Auftragsannahme
- Kommunikation über alle Dienste mit Unified Messaging Service
- Sichere Verbindung über IP (VPN)
- Zentrale Registrierung und Zuordnung der Verbindungskosten
- Alle integrierten Applikationen für den Teleworker verfügbar:
  – Voice Mail (nur HiPath 2030)



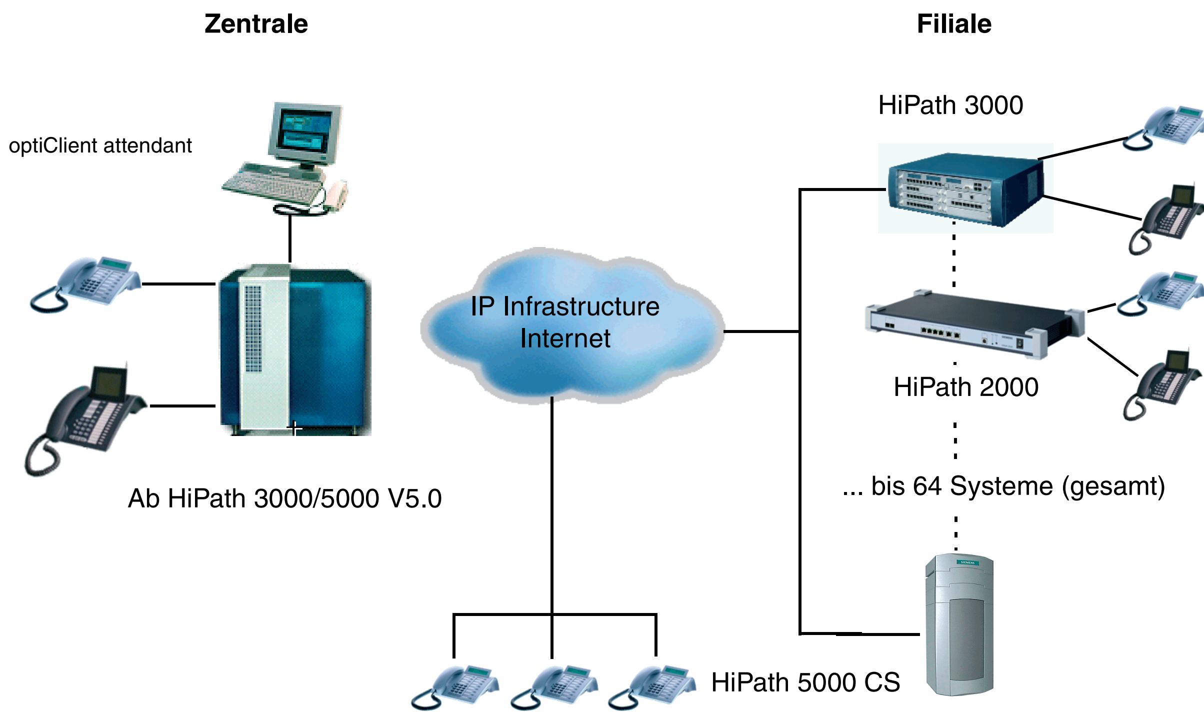
3.1.4.8 IP-Vernetzung mit mehreren HiPath 3000-Systemen und HiPath 2000

- HiPath ComScendo Service im Netz
- Vermittlung mit zentraler Belegtanzeige über alle Standorte
- Bis 64 Knoten
- Eine Infrastruktur für Sprache und Daten
- Payload Switching Any-to-Any



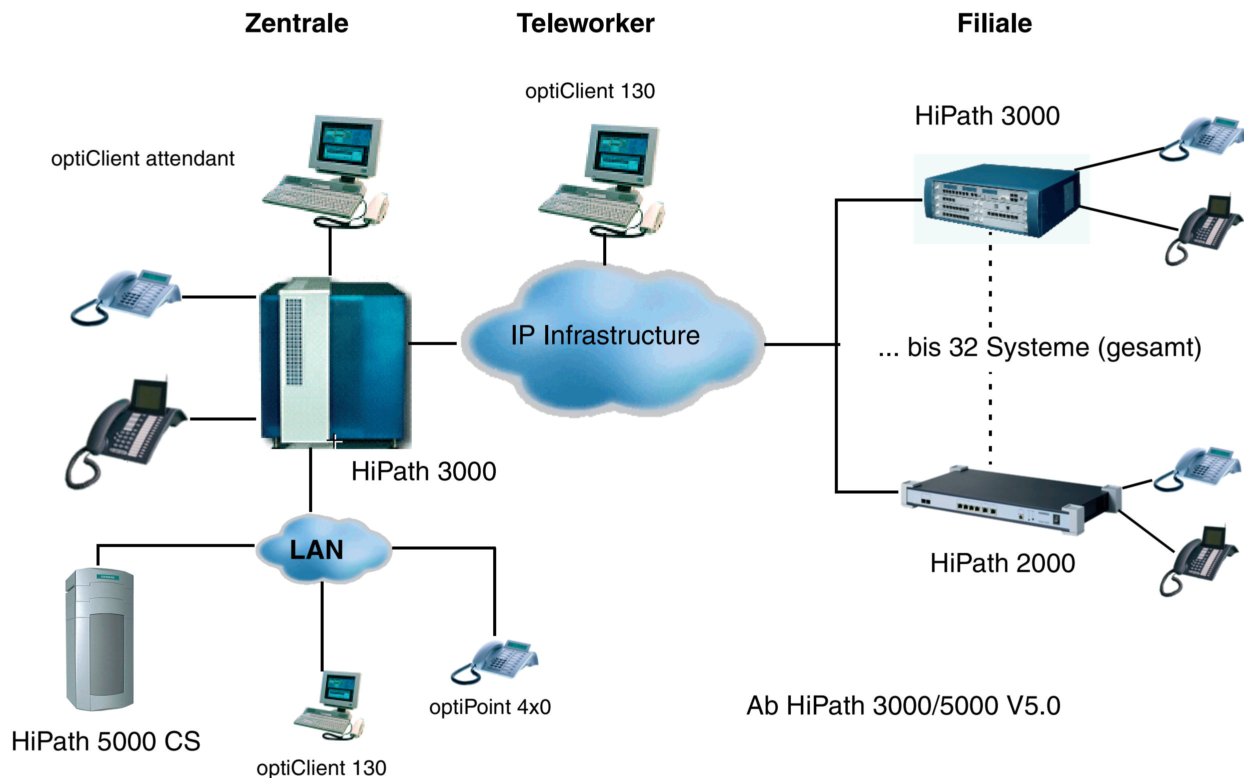
3.1.4.9 IP-Vernetzung HiPath 2000/3000 und HiPath 5000

- HiPath ComScendo Service im Netz
- Vermittlung mit zentraler Belegtanzeige über alle Standorte
- Bis 64 Knoten
- Eine Infrastruktur für Sprache und Daten
- Payload Switching Any-to-Any



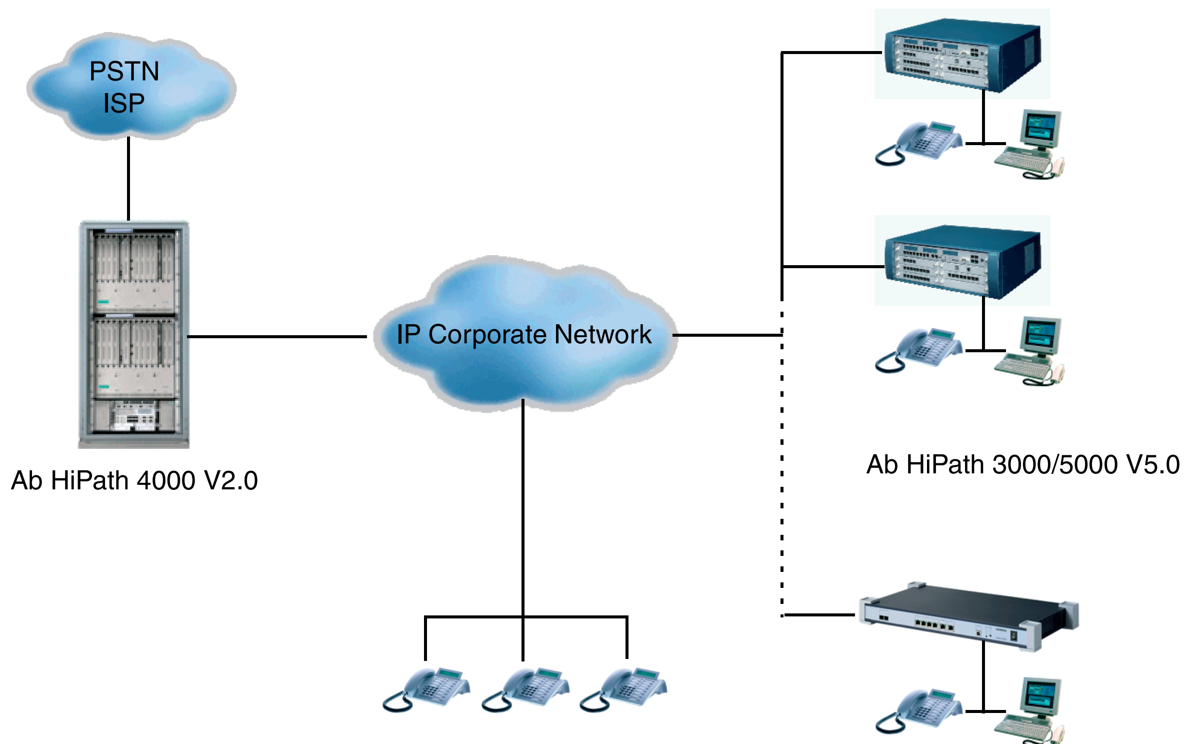
3.1.4.10 IP-Vernetzung über zentralen Applikations-Server HiPath 5000

- IP-Vernetzung mit bis 32 zu Knoten und 2000 Teilnehmern
- Bis zu sechs Vermittlungsplätze im Netz
- Zentrale Administration für das HiPath 3000/5000-Netz, lokale Administration der HiPath 2000 im Netz über WBM oder HiPath 2000/3000 Manager E
- Presence Manager für netzweite Leistungsmerkmale
- Einheitlicher, standortübergreifender Rufnummernplan mit offener und geschlossener Nummerierung
- Unified Messaging-Lösung
- Zentrales Accounting für Sprach- und Datenverkehr
- Payload Switching Any-to-Any; damit geringere Bandbreite, minimale Verzögerung und hohe Sprachqualität



3.1.4.11 IP-Vernetzung: Zentrale mit HiPath 4000 und Filialen mit HiPath 2000/3000

- Zentrales Fault Management
- Zentrales Accounting
- Netzweiter HiPath ComScendo Feature Set
- Einheitliche Infrastruktur für Sprache und Daten
- Payload Switching Any-to-Any; damit geringere Bandbreite, minimale Verzögerung und hohe Sprachqualität



3.1.4.12 Small Remote Site Konzept an HiPath 4000

- IP-Workpoints in einer Filiale sind zentral an der HiPath 4000 registriert
- Einheitliches HiPath 4000 User Interface für alle Netzteilnehmer
- HiPath 3000 oder HiPath 2000 als Survivable Media Gateway
- Notfallkonzept bei Netzwerkfehler sichert Erreichbarkeit und Verbindung zum PSTN
- Zentrale Applikationen verfügbar für Zentrale und Filiale
- Payload Switching Any-to-Any
- Maximaler Ausbau abhängig von HiPath 4000-Kriterien

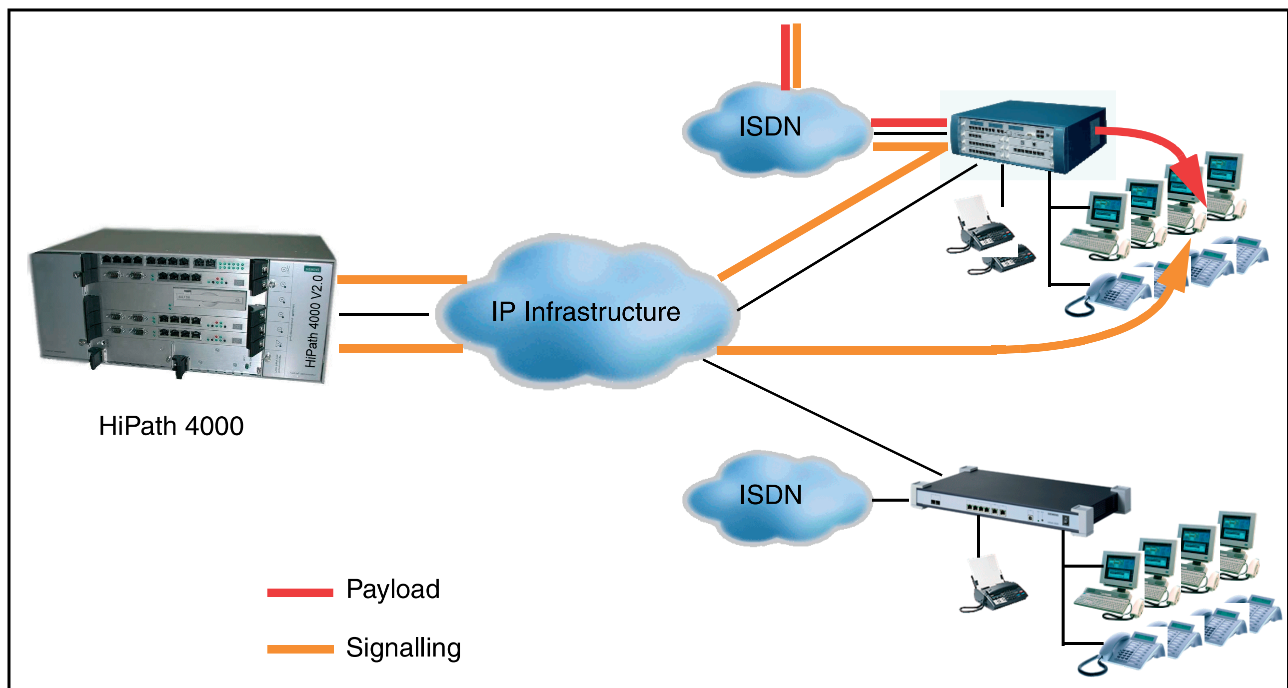


Bild 3-1 Signalisierung und Payload im Normalbetrieb

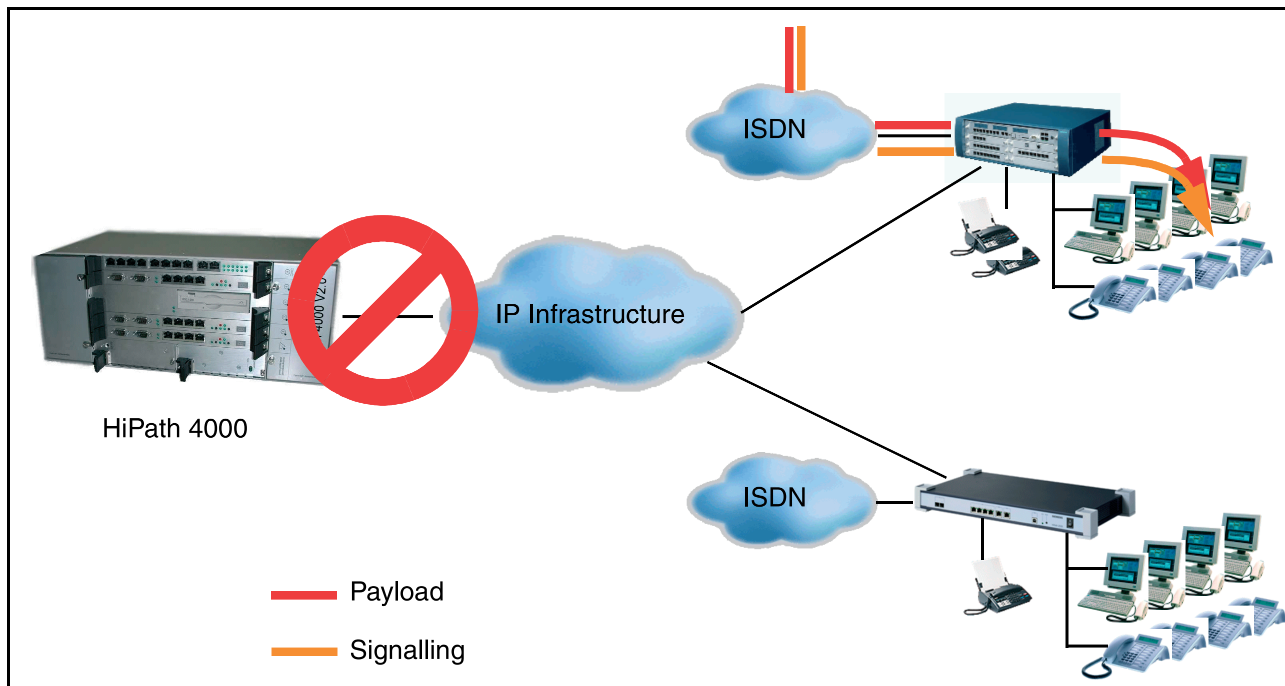
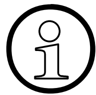


Bild 3-2 Signalisierung und Payload im Notbetrieb

3.2 SIP-Lösungen

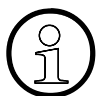


Informationen über SIP-Leistungsmerkmale finden Sie in der Leistungsmerkmalbeschreibung der HiPath 2000.

3.2.1 Internet Telefonie Service Provider (ITSP)

Der Markt der ITSP wächst rasant und damit die Vielzahl der angebotenen Leistungen und Geschäftsmodelle. HiPath 2000 unterstützt SIP-Provider-Anschlüsse mit Registrierung von Einzelrufnummern. Ab SMR 9 werden auch SIP-Anlagenanschlüsse für größere Systemausbauten unterstützt. Dem Kunden wird vom ITSP ein Rufnummernband bereitgestellt.

Damit eine sichere und hochqualitative Kommunikation gewährleistet ist, werden die HiPath Plattformen mit den ITSP-Schnittstellen intensiven Tests unterzogen.



Informationen über neue ITSPs erhalten Sie in der Release Note.

Unterstützte Leistungsmerkmale für Verbindungen zu ITSPs:

- CLIP/CLIR (Anzeige der Rufnummer des rufenden Teilnehmers beim gerufenen Teilnehmer / Unterdrückung der Rufnummer) ist vom Provider abhängig
- COLP/COLR (Anzeige der Rufnummer des gerufenen Teilnehmers beim rufenen Teilnehmer / Unterdrückung der Rufnummer) ist vom Provider abhängig
- Rückfrage, Übergabe, Halten

Folgende ITSPs sind an HiPath 2000 freigegeben:

Deutschland	QSC	Toplink	1&1	Freenet	Purtel	Sipgate	T-Online	X-SIP
DSL-Telefonie-Teilnehmeranschluss			X	X	X	X	X	X
DSL-Telefonie-Anlagenanschluss	X	X						X

Land	Italien	USA	
ITSP	Multilink	Cbeyond	Verizon
DSL-Telefonie-Teilnehmeranschluss	X		
DSL-Telefonie-Anlagenanschluss		X	X

Über die Freigabe weiterer ITSP werden Sie mit separater Vertriebinformation informiert. Die durch die Normierungsgremien SIP-Forum und ETSI/TISPAN erarbeiteten Standards, lassen den Herstellern bewusst Spielräume, um eine schnelle Entwicklung der neuen Technologie voranzutreiben. Darüber hinaus stellen die einzelnen Provider die Routing-Funktionen ihres Netzes auf das jeweilige Geschäftsmodell ab.

HiPath 2000 ermöglicht die Anbindung an ITSP für Standalone-Systeme und ab der Freigabe der HiPath 3000 V6.0 SMR 9 auch für vernetzte Systeme:

- Für das LCR werden bis zu vier gleichzeitig aktive SIP-Provider durch das System unterstützt.
- Maximal 4 gleichzeitige Verbindungen zum ITSP sind möglich.
- Bei DSL-Telefonie-Teilnehmeranschlüssen mit Einzelrufnummerregistrierung können bis zu 30 Benutzerkennungen (SIP Client User Accounts) eingerichtet werden.
- Sowohl S_0-Verbindungen als auch Verbindungen zum ITSP werden paralled über das Internet unterstützt.
- Bei allen Vernetzungslösungen (HiPath 2000 untereinander oder mit HiPath 3000) können sowohl S_0- als auch Amtszugänge zum ITSP verwendet werden. Die gleichzeitige Nutzung von Vernetzungen über CorNet-IP und ITSP-Anschlüsse wird ab der Freigabe der HiPath 3000 SMR 9 unterstützt.
- Internetzugänge: ADSL, SDSL

Systembedingte Anschaltebedingungen für DSL-Telefonie

Die HiPath 2000 kann auf zwei Arten Zugang zum Internet erlangen:

- Direkter Zugang zum Internet über die Anschaltung der HiPath 2000 an ein DSL-Modem. Die integrierten Firewalleinstellungen des Systems (NAT) stellen die Sicherheit bei direktem Zugang zum Internet für das Kundennetz sicher.
- Betrieb der HiPath 2000 im LAN hinter externen Router (ab SMR 9) mit Firewall- oder NAT-Funktion.

Grundsätzlich ist folgendes zu beachten:

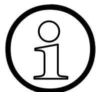
- Network Address Translation (NAT) ist die Umsetzung von IP-Adressen aus dem LAN für das Internet. NAT kann in der HiPath 2000 aktiviert und deaktiviert werden.
  Bestimmte Dienste, z. B. VoIP oder Bildtelefonie, betten allerdings die IP-Adressen der Teilnehmer in ihre Datenpakete ein (statt sie nur in den Paket-Headern zu vermerken). Solche Dienste sind nur innerhalb eines VPN mit NAT kompatibel oder bedürfen bei Verbindungen zu einem Internet Telefonie Provider den Einsatz zusätzlicher Protokolle (z. B. STUN) oder Infrastrukturkomponenten um Probleme mit NAT zu umgehen (=NAT Traversal).

- Bei Betrieb der HiPath 2000 hinter einem DSL-Modem, wird NAT Traversal im System umgesetzt.
- Für Szenarien in welchen die HiPath 2000 hinter einem Router/Firewall betrieben wird gilt:
  Stellt der ITSP einen STUN-Server für NAT Traversal bereit, so ist zu beachten, dass kein Router eingesetzt wird, der die "Symetric NAT“-Variante verwendet.

Bei ITSPs die NAT Traversal über Infrastrukturkomponenten im Providernetz wie z. B. Session Border Controllern (SBC) lösen, ist kein Eingriff in die Firewallkonfiguration oder die Verwendung des STUN Protokolls erforderlich.

„SIP-aware“ Firewalls besitzen ebenfalls eine NAT Traversal Funktion.

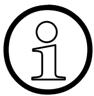
- Simple Traversal of UDP over NATs (STUN)
  STUN ist ein einfaches Client-/Server basiertes Netzwerkprotokoll welches das Vorhandensein von NAT-Firewalls und Routern erkennt. Ein STUN-Client auf der HiPath 2000 verbindet sich mit einem STUN-Server beim Internet Telephony Service Provider (ITSP). Der STUN-Server liefert Informationen, wie der Internetanschluss von außen gesehen wird. Diese werden von der HiPath 2000 für den Versand von Paketen zu einem ITSP oder Gesprächspartner im Internet genutzt, um die HiPath 2000 auch hinter einem NAT-Gerät aus dem Internet erreichbar zu machen. Die Einstellungen einer vorgelagerten NAT-Firewall oder eines NAT-Routers müssen dadurch nicht geändert werden.
- Sonderrufnummern / Notrufe / Faxe
  - Sonderrufnummern werden nicht von allen ITSPs weitergeleitet. Die HiPath 2000 routet eine Auswahl von Sonderrufnummern per Default über ISDN:
    0137 Televoting
    0138 Televoting
    0900 Premium-Rate Dienste
    118xy Auskunftsdienst
    116 116 Sperrnotrufnummer für EC-Karten, Kreditkarten usw.
    Für das Führen von Amtsgesprächen zu ausgewählten Service Providern/Service Diensten (z. B. 0180, 0800 ect.) ist das LCR gemäß den Anforderungen vom Service anzupassen.



Sollte eine Anlage ausschließlich über einen DSL-Anschluss betrieben werden, so kann das Routing von Notruf-, Sonderrufnummern auch zum ITSP konfiguriert werden. Es ist vorher unbedingt zu prüfen, dass der ITSP diese Dienste unterstützt.

  - Notrufnummern (110, 112) werden nur teilweise von den ITSPs unterstützt, da beim Ausstieg in das öffentliche Netz das Ortsnetz nicht eindeutig zugeordnet werden kann. Diese Verbindungen müssen über S_0-Zugänge realisiert und standardmäßig durch Defaulteinträge im LCR vorgeleistet werden.

HiPath 2000 routet daher per Default alle Sonderufnummern und Notrufnummern über ISDN. Auch analoge Teilnehmer (2 x a/b für Fax oder Modem) werden per Default über ISDN geroutet.



Sollte die Anlage ausschließlich über einen DSL-Anschluss betrieben werden, so kann das Routing von Notruf-, Sonderrufnummern auch zum ITSP konfiguriert werden. Es ist vorher unbedingt zu prüfen, dass der ITSP diese Dienste unterstützt.

- Bandbreitenkontrolle

  Jede Verbindung zum SIP-Provider belegt DSP-Ressourcen der HiPath 2000, ähnlich der Verbindungen mit analog/IP-Übergang (z.B. ISDN-Verbindungen) oder bei Nutzung von Music On Hold. Im praktischen Einsatz wird daher empfohlen, die HiPath 2000 mit maximal 2 gleichzeitigen ITSP-Providerverbindungen zu betreiben und weitere Amtszugänge über ISDN-Anschlüsse zu realisieren. Beachten Sie bitte die Hinweise in Abschnitt 1.5.3.2 Dynamische Ausbaugrenzen.

  Bei Anschlüssen, die nicht QoS-fähig sind, (in der Regel bei ADSL-Anschlüssen) sind Einschränkungen bei der Sprachqualität möglich. Eine gute Sprachqualität wird i.d.R. erzielt wenn ein nicht QoS-fähiger DSL-Anschluss ausschließlich für Sprachverbindungen zum ITSP genutzt wird.

  Bedingt durch die Netzverfügbarkeit der Provider sind temporäre Störungen der Verbindungen möglich. Bitte beachten Sie die Geschäftsbedingungen der ITSP. Sollten Verbindungen über SIP nicht zustande kommen, werden diese durch HiPath 2000 über ISDN aufgebaut.

  Der beim Kunden eingesetzte Router muss zur Sicherstellung einer gute Sprachqualität über QoS Funktionen und Bandbreitenkontrollmechanismen bereitstellen.

- Rufnummernanzeige

  Die Leistungsmerkmale CLIP und CLIR sind bei den einzelnen ITSPs unterschiedlich implementiert. Einschränkungen bei der Rufnummernanzeige bzw. Einträgen in Anruferlisten sind möglich. Das Leistungsmerkmal CLIP no Screening wird nicht von jedem ITSP unterstützt. Im Display/Anruferliste des B-Teilnehmers erscheint die Rufnummer der Leitung zum ITSP und nicht die Rufnummer des rufenden A-Teilnehmers.

- Verbindungen mit Ausstieg ins Festnetz/Mobilfunk oder aus dem Festnetz/Mobilfunk kommend

  – Provider-interne Verbindungen (Ziel ist besetzt/nicht registriert)
    Interne Verbindungen zu einem besetzten oder nicht registrierten Teilnehmer werden im Regelfall korrekt signalisiert.

- Rufe zu anderen Providern
  Diese Rufe sind technisch möglich, jedoch stellen die einzelnen Provider die Routing-Funktionen ihres Netzes auf das jeweilige Geschäftsmodell ab. Nähere Informationen sind beim jeweiligen ITSP einzuholen.

- MFV-Übertragung über IP
  MFV-Zeichen werden im Sprachkanal übertragen. Die sichere Übertragung erfordert den Codec G.711 zum Provider.

- Fax-Übertragungen
  Fax-Übertragungen werden nicht von jedem Provider unterstützt. Es wird empfohlen, wie standardmäßig eingestellt Fax-Übertragungen über ISDN zu realisieren. Seitens HiPath 2000 sind Fax-Übertragungen bei DSL-Telefonieanschlüsse über G.711-Gateway-Kanäle möglich. T.38 zu ITSPs wird nicht unterstützt.

- Modem-Übertragungen und ISDN-Datendienste (z. B. Nutzung von EC Cash-Geräten) werden nicht unterstützt.

- CSTA-Monitoring von Anschlüssen zu ITSPs wird nicht unterstützt.
  Dadurch ist eine Nutzung von Applikationen, die dieses vorsehen, nicht möglich (z. B. Call Center).

- Gesprächsdatenauswertung
  Über das SIP Protokoll werden Einzelgesprächsdaten nach Zeit aufgezeichnet und sind über externe Applikationen wie z.B. Teledata Office auswertbar.

3.3 Dienstleistungen

3.3.1 HiPath Netzwerkanalyse

Für die Vermarktung von HiPath 2000 Standalone-Systemen wird eine vereinfachte Netzwerkanalyse gemäß Checkliste durchgeführt.

Für den Betrieb von HiPath 2000-Systemen in HiPath 3000/5000-Netzen gelten die gleichen Voraussetzungen, wie in HiPath 3000/5000 ab V5.0 festgelegt.

Weitere Informationen dazu finden Sie über die Homepage der **HiPath Netzwerkanalyse V2.0**. Von dort kann zu der Vertriebsinformation, der Service Richtlinie, sowie dem Leitfaden verzweigt werden.

Die beschriebenen Dienstleistungen im Zusammenhang mit HiPath IP-Konvergenzlösungen wurden im Rahmen von Markteinführungsaktivitäten durch Com ESR VAS PS mit einer separaten Vertriebsfreigabe sukzessive in die Vertriebsorganisationen eingeführt. Weitere grundsätzliche Informationen zu Com ESR VAS PS und der Markteinführung von Professional Services sind unter den aufgeführten Intranetadressen zu finden.

3.4 Technische Konzepte

3.4.1 Umgebungsanforderungen für VoIP

Um die Qualität der Sprachübertragung sicherzustellen, müssen die verwendeten Netzwerke bestimmte Anforderungen erfüllen, die insbesondere für die Vermeidung inakzeptabler Verzögerungen wichtig sind.

3.4.1.1 Umgebungsanforderungen im LAN

- LAN mit 10/100/1000 MBit/sec
- Eigener Port am Switch oder Router für jede beteiligte Komponente im IP-Netz (keine HUB's als Konzentrator)
- Höchstens 50 ms Verzögerung in einer Richtung (One Way Delay); höchstens 150 ms Gesamtverzögerung
- Höchstens 3% Paketverlust
- Höchstens 20 ms Jitter
- Unterstützung für Quality of Service (QoS) – IEEE 802.p, DiffServ (RFC 2474) oder ToS (RFC 791)
- Höchstens 40% Netzwerkauslastung

3.4.1.2 Zusätzliche Randbedingungen im WAN

Wenn VoIP in LANs, die über WANs gekoppelt sind, LAN-übergreifend eingesetzt wird, gelten folgende Mindestanforderungen:

- Die LANs müssen jeweils über einen WAN-Anschluss mit fester IP-Adresse mit dem Internet verbunden sein.
- Die für die Gespräche benötigte Bandbreite muss jederzeit sowohl im Up- und Download zur Verfügung stehen.
- Die max. Anzahl der simultanen VoIP-Verbindungen über WAN ergibt sich u.a. in Abhängigkeit der verwendeten Codecs.
- Zu den WAN-Verbindungen zählen neben DSL z.B. auch Richtfunk- und Laserlinkstrecken
- HiPath 2000 hat kein integriertes Modem, d.h. es ist ein externes Modem erforderlich (z.B. DSL-Modem)

- Wenn die HiPath 2000 an einer Schnittstelle (WAN oder PPP/ISDN) das **NAT** Flag gesetzt hat, dann ist die HiPath 2000 sowie auch das lokale LAN geschützt.
  Hinweis: Bei aktiven VPN werden die notwendigen Ports UDP 500 & 4500 an dem Interface automatisch geöffnet.

3.4.1.3 Quality of Service

Quality of Service umfasst verschiedene Methoden, in IP-Netzen gewisse Eigenschaften der Übertragung sicherzustellen. Die genannten Standards definieren Prioritätsklassen zur Übertragung von Daten. Damit können aktive Netzkomponenten (Switches, Router) VoIP-Datenpakete gegenüber klassischen Datenpaketen priorisiert übertragen. Delay und Jitter sind im wesentlichen von den Übertragungseigenschaften der Netzwerkkomponenten abhängig. Wenn mehrerer Applikationen gleichberechtigt über IP arbeiten, müssen diese sich die vorhandene Bandbreite teilen. Insbesondere im WAN ist daher die maximale Anzahl simultaner VoIP-Verbindungen anhand von Codecvorgaben und vorhandener Bandbreite zu planen. Hohe Werte für Paketverluste, Delay und Jitter sind im wesentlichen die Ursache für schlechte Sprachqualität.

3.4.2 Bandbreitenbedarf in LAN/WAN-Umgebungen

Die HiPath 2000 ist auf Optimierung der Bandbreitennutzung ausgelegt. Es implementiert dazu unter anderem folgende Funktionen:

- Stille-Unterdrückung
- Entdeckung und Unterdrückung von Hintergrundgeräuschen
- dynamische Feststellung von Sprache und Fax

Verfügbare Bandbreite

Die für Sprache benötigte Bandbreite muss im Netzwerk jederzeit verfügbar sein. Dazu sind vor der Installation der Komponenten Netzwerk-Mess- und -Analyseverfahren erforderlich.

Payload-Verbindungen mit RTP (Realtime Transport Protocol) in einer LAN-Umgebung:

Die erforderliche Bandbreite für Sprachübertragung in einem IP-Netzwerk lässt sich mit Hilfe der folgenden Tabelle berechnen:

Codec-Typ	Paketierungs-Parameter	Paketabstand/ Rahmengröße (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	Ethernet Load (inkl.) Kopf (kBit/s)
G.711	20	20	160	230	44%	92

Tabelle 3-1 Bandbreitenbedarf nach Codec

Codec-Typ	Paketie-rungs-Parameter	Paket-abstand/ Rahmen-größe (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	Ethernet Load (inkl.) Kopf (kBit/s)
G.711	30	30	240	310	29%	82,7
G.711	40	40	320	390	22%	78
G.711	60	60	480	550	15%	73,3
G.723.1	1	30	24	94	292%	25,1
G.723.1	2	60	48	118	146%	15,7
G.729A	1	20	20	90	350%	36
G.729A	2	40	40	110	175%	22
G.729A	3	60	60	130	117%	17,3
RTCP		5000		280		0,4

Tabelle 3-1 Bandbreitenbedarf nach Codec

Der Load im LAN ist für eine Richtung kalkuliert. Für Payload-Verbindungen in beide Richtungen ist die doppelte Bandbreite erforderlich. Mit HiPath 2000 wird VAD mit Codec G.7231A und G.729AB unterstützt. Werden diese Codes verwendet, nimmt die Bandbreitenanforderung abhängig vom Umfang der Ruheperioden in Sprachsignalen ab.

Die Berechnung schließt VLAN-Tagging entsprechend IEEE 802 1q ein. Ohne VLAN-Tagging ist die Länge eines Pakets um 4 Bytes kürzer.

Der Overhead berechnet sich wie folgt:

Protokoll	Bytes
RTP-Header	12
UDP-Header	8
IP-Header	20
802.1Q VLAN Tagging	4
MAC (incl. Preamble, FCS)	26
Summe	**70**

Tabelle 3-2 Overhead-Berechnung

Report-Typ	Report-Intervall (s)	Durchschnittl. Ethernet-Paketgröße (Bytes)	EthernetLoad (inkl.) Kopf (kBit/s)
Sender-Report	5	140	0,2
Empfänger-Report	5	140	0,2
Summe			**0,4**

Tabelle 3-3 Kontrolle Payload-Verbindung mit parallelem RTCP (Real-time Transport Control Protocol)

Payload-Verbindungen mit RTP (Realtime Transport Protocol) in einer WAN-Umgebung:

Für Payload-Verbindungen mit RTP (Realtime Transport Protocol) in einer WAN-Umgebung errechnen sich folgende Werte:

Codec	Paketierungs-Parameter	Paketabstand/ Rahmengröße (ms)	Payload (Bytes)	Paketlänge (Bytes)	Payload-Paket (Overhead in %)	WAN Load (kBit/s)	Paketlänge mit Header-Kompression (Bytes)	WAN Load mit Header-Kompression (kBit/s)
G.711	20	20	160	206	29%	82,4		
G.711	30	30	240	286	19%	76,3		
G.711	40	40	320	366	14%	73,2		
G.711	60	60	480	526	10%	70,1		
G.723.1	1	30	24	70	192%	18,7	32	8,5
G.723.1	2	60	48	94	96%	12,5	56	7,5
G.729A	1	20	20	66	230%	26,4	28	11,2
G.729A	2	40	40	86	115%	17,2	48	9,6
G.729A	3	60	60	106	77%	14,1	68	9,1
RTCP		5000		230		0,4		0,4

Tabelle 3-4 WAN-Bandbreitenbedarf nach Codec

Der WAN-Load ist für eine Richtung kalkuliert. Da WAN-Kanäle gewöhnlich Kanäle in beide Richtungen beinhalten, ist dies gleichbedeutend mit der erforderlichen Bandbreite für z.B. einen ISDN-Kanal.

Der Overhead berechnet sich wie folgt:

Protokoll	**Bytes**
RTP-Header	12
UDP-Header	8
IP-Header	20
PPP	9
Summe	**46**
Komprimierte Header	**8**

Tabelle 3-5 Overhead-Berechnung

Für RTP/UDP/IP-Header-Kompression wird gewöhnlich ein „komprimierter Header“ verwendet. Zusätzlich wird alle 5 Sekunden ein voller Header (46 Bytes) gesendet.

Die Daumenregel zum Berechnen der erforderlichen Bandbreite für n parallele VoIP-Verbindungen mit G.711 (ein Frame pro RTP-Paket) lautet:

$\text{Bandbreite}_{LAN} = n \times (180_{\text{Voice-Payload}} + 0{,}4_{\text{RTPC}})$

$\text{Bandbreite}_{WAN} = n \times (82_{\text{Voice-Payload}} + 0{,}4_{\text{RTPC}})$

Bei anderen Codecs oder Paketwerten wechseln die Annäherungswerte für Sprach-Payload. Ferner muss die Bandbreite für Gebühreninformationen und andere Anwendungen berücksichtigt werden.

Bandbreitenanforderungen für CAR-Alive / Node Survey

Für CAR-Alive / Node Survey (PBX-Knotenüberwachung) gibt es zwei verschiedene Methoden: entweder ein TCP-basierter Mechanismus, oder ein ICMP-Ping (konfigurierbar über Manage I oder WBM).

Node-Anzahl	**TCP-Load (kBit/s)**	**Ping-Load (kBit/s)**	**Zeit-intervall**
1	0,1	0,1	12
2	0,2	0,3	
3	0,5	0,8	
4	1,0	1,7	
5	1,7	2,8	
6	2,5	4,2	

Tabelle 3-6 LAN-Bandbreitenbedarf für CAR-Alive / Node Survey

Node-Anzahl	TCP-Load (kBit/s)	Ping-Load (kBit/s)
1	0,07	0,11
2	0,14	0,22
3	0,41	0,66
4	0,82	1,31
5	1,37	2,19
6	2,06	3,28

Tabelle 3-7 WAN-Bandbreitenbedarf für CAR-Alive / Node Survey

Die Daumenregel zum Berechnen der erforderlichen Bandbreite für CAR-Alive zwischen n Knoten lautet:

$$\textbf{Bandbreite}_{\textbf{LAN}} = \textbf{n} \times \textbf{(n-1)} \times \textbf{Bytes}_{\textbf{AliveMsg}} \times \textbf{8} \div \textbf{1000} \div \textbf{T}_{\textbf{Timeout between ping}}$$

Der Wert für $\textbf{Bytes}_{\textbf{AliveMsg}}$ beträgt:

im LAN **212** mit PING, oder **127** mit TCP
im WAN **188** mit PING, oder **102** mit TCP

Der Default-Timeout zwischen zwei Pings beträgt 12 Sekunden.

Bandbreitenbedarf in LAN-Umgebungen mit Verschlüsselung

Verschlüsselung erfordert eine erhöhte Bandbreite. In den nachfolgenden Tabellen werden die erforderlichen Bandbreiten abhängig von den möglichen Sprach-Codecs und Verschlüsselungs-Algorithmen für Ethernet-Pakete aufgelistet. Die Verschlüsselung erfolgt durch einen IPsec-Protokollstack. Von den unterschiedlichen, bei IPsec möglichen Operationsmodi wird hier nur eine betrachtet: der ESP-Tunnelmodus mit Authentifizierung.

Dieser Operationsmodus bietet die höchste Sicherheit für Site-to-Site-VPNs.

Protokoll	Bytes	verschlüsselt?
ESP Trailer	12	
ESP Padding	variierend (**y**)	verschlüsselt
ESP Padding Header	2	verschlüsselt
Voice Paload	variierend (**x**)	verschlüsselt
RTP	12	verschlüsselt

Tabelle 3-8 Struktur eines verschlüsselten Voice-Pakets (ESP-Tunnelmodus mit Authentifizierung)

Protokoll	**Bytes**	**verschlüsselt?**
UDP	8	verschlüsselt
IP (original)	20	verschlüsselt
ESP Header	8 + **IV**[1]	
IP (Tunnel)	20	
802.1Q VLAN Tagging	4	
MAC (incl. Preamble, FCS)	26	
Summe	**112 + IV + x + y**	

Tabelle 3-8 Struktur eines verschlüsselten Voice-Pakets (ESP-Tunnelmodus mit Authentifizierung)

1 IV = Initialisierungsvektor. Erläuterung siehe Text unterhalb der Tabelle

ESP-Header-Länge: Die Länge des ESP-Headers hängt vom verwendeten Verschlüsselungs-Algorithmus ab. Bei Verwendung für Cipher Block Chaining (Blockverschlüsselung) enthält der ESP-Header einen Initialisierungsvektor (in der Tabelle weiter oben mit „IV“ bezeichnet). Die Länge des Initialisierungsvektors ist gleich der Länge eines Verschlüsselungsblocks.

Auffüllen (Padding): Ein Auffüllen mit Bytes ist nötig, da die Verschlüsselungs-Algorithmen auf Blockverschlüsselung basieren. Der gesamte verschlüsselte Anteil des Pakets (Original-IP/UDP/RTP-Header, Voice Payload, ESP Padding Header, ESP Padding) muss ein Integer-Wert sein, der ein Vielfaches der Verschlüsselungs-Blocklänge beträgt.

Verschlüsselungs-Algorithmus	**Blocklänge**	**Länge Initialisierungsvektor**
AES	16 Byte (128 Bit)	16 Byte (128 Bit)
DES	8 Byte (64 Bit)	8 Byte (64 Bit)
3DES	8 Byte (64 Bit)	8 Byte (64 Bit)

Tabelle 3-9 Blocklängen der Verschlüsselungs-Algorithmen

Die Anzahl der benötigten Auffüll-Bytes für Voice-Pakete errechnet sich aus folgender Formel:

(42 + x + y) [Bytes] = N x (8 oder 16 [Bytes]) // N ist ein Integer.

Bandbreitenkalkulation für den AES-Verschlüsselungs-Algorithmus:

Codec	**Paketierung**	**Beispielgröße (ms)**	**Payload (Bytes)**	**Padding (Bytes)**	**Ethernet Paketlänge**	**Payload-Paket (Overhead in %)**	**Ethernet Load inkl. Präambel (kBit/s)**
G.711	20	20	160	6	**294**	75%	**117,6**

Tabelle 3-10 LAN-Bandbreitenbedarf bei AES-Verschlüsselung – nach Codec

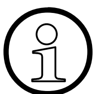
Codec	Pake-tierung	Beispiel-größe (ms)	Pay-load (Bytes)	Padding (Bytes)	Ethernet Paket-länge	Payload-Pa-ket (Over-head in %)	Ethernet Load inkl. Präambel (kBit/s)
G.711	30	30	240	6	**372**	50%	**99,2**
G.711	40	40	320	6	**454**	38%	**90,8**
G.711	60	60	480	6	**614**	25%	**81,9**
G.723.1	1	30	24	**14**	**166**	500%	**44,3**
G.723.1	2	60	48	6	**182**	250%	**24,3**
G.729A	1	20	20	2	**150**	600%	**60,0**
G.729A	2	40	40	**14**	**182**	300%	**36,4**
G.729A	3	60	60	**10**	**198**	200%	**26,4**

Tabelle 3-10 LAN-Bandbreitenbedarf bei AES-Verschlüsselung – nach Codec

Bandbreitenkalkulation für den DES/3DES-Verschlüsselungs-Algorithmus:

Codec	Pake-tierung	Beispiel-größe (ms)	Pay-load (Bytes)	Padding (Bytes)	Ethernet Paket-länge	Payload-Pa-ket (Over-head in %)	Ethernet Load inkl. Präambel (kBit/s)
G.711	20	20	160	6	**286**	75%	**114,4**
G.711	30	30	240	6	**366**	50%	**97,6**
G.711	40	40	320	6	**446**	38%	**89,2**
G.711	60	60	480	6	**606**	25%	**80,8**
G.723.1	1	30	24	**6**	**150**	500%	**40,0**
G.723.1	2	60	48	6	**174**	250%	**23,2**
G.723.1	**3**	**90**	**72**	**6**	**198**	**167%**	**17,6**
G.729A	1	20	20	2	**142**	600%	**56,8**
G.729A	2	40	40	**6**	**166**	300%	**33,2**
G.729A	3	60	60	**2**	**182**	200%	**24,3**

Tabelle 3-11 LAN-Bandbreitenbedarf bei DES/3DES-Verschlüsselung – nach Codec


Werte, die sich in den beiden Tabellen unterscheiden, sind hervorgehoben.

3.4.3 Bandbreitenbedarf für VoIP über die DSL-Telefonieanschlüsse

Die folgende Tabelle gibt an, wie viele Sprachkanäle rein rechnerisch zur gleichen Zeit mit den jeweiligen Bandbreiten übertragen werden können.

Rechnerische Werte:			**ADSL 1000**	**ADSL 2000**	**ADSL 6000**	**SDSL 1000**	**SDSL 2000**
Uplink (kbps) Downlink (kBit/s)			128 1000	192 2000	576 6000	1024 1024	2048 2048
Codec	Sample size (ms)	ca. Bandbreite pro Gespräch (kBit/s)	Anzahl der max. gleichzeitigen Gespräche				
G.711	20	94	1	2	6	10	21*
G.711	40	79	1	2	7	12	25*
G.711	60	74	1	2	7	13	27*
G.723	30	26	4	7	22*	30**	30**
G.723	60	16	8	12	30**	30**	30**
G.729	20	38	3	4	15	26	30**
G.729	40	23	5	8	24*	30**	30**
G.729	60	18	7	10	30**	30**	30**
* max. 20 für HiPath 2020 ** max. 30 limitiert durch HiPath 2030							

Die Auswahl der Bandbreite des xDSL-Anschlusses wird bestimmt durch die Summe der zu realisierenden Daten- und Sprachdienste. Zu beachten ist der technologiebedingte maximale Datendurchsatz der HiPath 2000 für das Daten-Routing (ausbauabhängig).

Provider- und tarifanhängig kann bei Überschreiten eines bestimmten Datenvolumens eine Drosselung des Up- und Downlinks durch den ITSP erfolgen.

3.5 Erfüllte Standards für HiPath 2000 V1.0

- **Ethernet**
  - RFC 894 Ethernet II Encapsulation
  - IEEE 802.1Q Virtual LANs
  - IEEE 802.2 Logical Link Control
  - IEEE 802.3u 100 BASE-T
  - IEEE 802.3x Full Duplex Operation
- **IP / Routing**

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 2822 Internet Message Format
- RFC 826 ARP
- RFC 2131 DHCP
- RFC 1918 IP Addressing
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1618 PPP over ISDN
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1877 PPP Internet Protocol Control Protocol
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake AuthenticationProtocol (CHAP)
- RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)

- **NAT**
  - RFC 2663 NAT
- **IPSec**
  - RFC 2401 Security Architecture for IP
  - RFC 2402 AH - IP Authentication Header
  - RFC 2403 IPsec Authentication - MD5
  - RFC 2404 IPsec Authentication - SHA-1
  - RFC 2405 IPsec Encryption - DES
  - RFC 2406 ESP - IPsec encryption
  - RFC 2407 IPsec DOI
  - RFC 2408 ISAKMP
  - RFC 2409 IKE

  - RFC 2410 IPsec encryption - NULL
  - RFC 2411 IP Security Document Roadmap
  - RFC 2412 OAKLEY
- **SNMP**
  - RFC 1213 MIB-II
- **QoS**
  - IEEE 802.1p Priority Tagging
  - RFC 1349 Type of Service in the IP Suite
  - RFC 2475 An Architecture for Differentiated Services
  - RFC 2597 Assured Forwarding PHB Group
  - RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)
- **SIP-Telefonie**
  - RFC 2327 SDP: Session Description Protocol
  - RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
  - RFC 2782 DNS RR for specifying the location of services (DNS SRV)
  - RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
  - RFC 3261 SIP: Session Initiation Protocol
  - RFC 3262 Reliability of Provisional Responses in the Session Initiation Protocol (SIP) / Early Media
  - RFC 3263 SIP Loating Servers
  - RFC 3264 Offer/Answer Model with the Session Description Protocol
  - RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
  - RFC 3550 RTP: Transport Protocol for Real-Time Applications
- **other**
  - RFC 959 FTP
  - RFC 1305 NTPv3
  - RFC 1889 RTP
  - RFC 2833 RTP Payload for DTMF Digits

- RFC 3544 IP Header Compression over PPP
- RFC 3605 Real Time Control Protocol (RTCP)
- RFC 1951 DEFLATE
- DNS

3.6 Quality of Service (QoS)

Quality of Service umfasst verschiedene Methoden, in paketorientierten Netzen (IP) gewisse Eigenschaften der Übertragung sicherzustellen.

So ist es zum Beispiel für Voice over IP wichtig, eine Mindestbandbreite für die Dauer der Übertragung sicherzustellen. Wenn mehrere Applikationen gleichberechtigt über IP arbeiten, so wird die vorhandene Bandbreite einer Übertragungsstrecke (z. B. ein ISDN-B-Kanal, 64kBit/s) aufgeteilt, so dass unter Umständen eine Sprachverbindung von Paketverlusten betroffen ist, woraus eine schlechte Sprachqualität resultieren kann.

Die HiPath 2000 verwendet verschiedene Verfahren zur Realisierung von Quality of Service.

Auf der Schicht 2 (nach OSI, Ethernet) kann eine Erweiterung (IEEE 802.1p) gegenüber dem Standard-Ethernet-Format (DIX V2) aktiviert werden, die den Ethernet-Header um einige Informationen erweitert, unter anderem um ein drei Bit breites Datenfeld. Mit diesem Feld wird dem Datenpaket eine Priorisierungsinformation mitgegeben. Für alle Pakete, die die Baugruppe aus dem LAN erreichen, werden beide Ethernet-Formate (IEEE 802.1p und DIX V2) verstanden, für alle Pakete, die von der Baugruppe ins LAN verschickt werden, kann das Format ausgewählt werden. Bevor dieser Parameter aktiviert wird, sollte geprüft werden, ob alle Komponenten im Netzwerk dieses Format unterstützen. Andernfalls ist unter Umständen vom LAN aus kein Zugang auf die HiPath 2000 mehr möglich.

Beim Übergang auf ein anderes Transportmedium (z. B. ISDN) wird der Ethernet-Header nicht weitertransportiert. Ein IP-Router (wie der der HiPath 2000) kann allerdings die Informationen zur Priorisierung nutzen, die im IP-Header enthalten sind. Die Priorisierung auf IP-Ebene können aber auch reine IP-Router nutzen, die zum Beispiel zwei Netzsegmente miteinander verbinden. Als QoS-Verfahren werden entweder drei Bit (IP-Präzedenz nach RFC 791, älterer Standard) oder sechs Bit (Differentiated Services oder DiffServ, nach RFC 2474) zur Bildung von unterschiedlichen Klassen ausgewertet. Der IP-Router der HiPath 2000 stellt diesen Klassen unterschiedliche Bandbreiten zur Verfügung, so dass etwa Sprachpakete vorrangig behandelt werden können.

Für das DiffServ-Verfahren werden verschiedene sogenannte Codepunkte („Grundeinstellungen > AF/EF-Codepunkte“) definiert und anhand dieser Codepunkte zwei verschiedene Verfahren für die Behandlung der Payload verschieden markierter Datenströme genutzt:

Das Verfahren „Expedited Forwarded“ (EF) – nach RFC 2598 – garantiert eine konstante Bandbreite für die Daten dieser Klasse. Wird der definierte Wert erreicht, werden alle Pakete, die diese Bandbreite überschreiten würden, verworfen. Auf der HiPath 2000 ist für EF eine eigene Klasse definiert. Für diese Klasse kann die Bandbreite für jeden ISDN-Partner in Prozent definiert werden (QoS-Bandbreite für EF).

Das Verfahren „Assured Forwarding“ (AF) – nach RFC 2597 – garantiert eine minimale Bandbreite für die Daten einer (von mehreren) Klassen. Die Klassen niedrigerer Priorität teilen sich jeweils die von EF bzw. den höher priorisierten Klassen nicht genutzte Bandbreite. Innerhalb jeder Klasse kann über den Dropping Level zusätzlich definiert werden, wie schnell Pakete ver-

worfen werden sollen, wenn sie nicht schnell genug weitertransportiert werden können. So ist es bei Sprachpaketen nicht sinnvoll, sie lange zwischenzuspeichern (dadurch erhöht sich nur das Delay, die Verzögerung). Bei einer gesicherten Datenübertragung (z. B. einem Dateitransfer) ist es hingegen vorteilhaft, einen größeren Zwischenspeicher zu haben, da es andernfalls ohnehin zu Paketwiederholungen zwischen den beiden Endstellen kommen würde.

Auf der HiPath 2000 sind vier Klassen für AF reserviert: AF1x (hohe Priorität), AF2x, AF3x und AF4x (niedrige Priorität), wobei „x“ für einen von drei Dropping-Stufen steht: niedrig (1), mittel (2) und hoch (3). Bei „niedrig“ werden Pakete lange zwischengespeichert, bei „hoch“ werden Pakete früh verworfen, wenn sie nicht weitertransportiert werden können. Unmarkierte IP-Pakete (ToS-Feld=00) werden mit niedrigster Priorität behandelt.

Wenn ein Routing-Partner nur mit einem der beiden Standards (DiffServ oder IP-Präzedenz) arbeiten kann (z. B. ein älterer Router, der nur mit IP-Präzedenz arbeitet), so kann die HiPath 2000 das ToS-Feld entsprechend übersetzen. Dies kann bei jedem PSTN-Partner bzw. bei der LAN-Schnittstelle eingestellt werden. Im Default „identisch“ wird nichts übersetzt, mit den beiden Werten „DiffServ“ bzw. „IP-Präzedenz“ findet jeweils eine Übersetzung gemäß der untenstehenden Tabelle statt, wenn das Feld nicht nach dem eingestellten Standard versorgt ist.

Bei IP-Datenverkehr werden die IP-Pakete, die die HiPath 2000 selbst generiert, in fünf Gruppen aufgeteilt (z. B. der H.323-Gateway). Für vier dieser Gruppen kann eingestellt werden, mit welchem Codepunkt die Pakete markiert werden sollen.

- Voice-Payload für die Voice over IP-Telefonie
- Call Signaling für den Verbindungsaufbau bei Voice over IP
- Data Payload zum Beispiel für IP-Vernetzung mit Fax oder Modem
- Network Control zum Beispiel SNMP-Traps

Der übrige Datenverkehr wird mit „deaktiviert“, also 00 markiert.

Der Zusammenhang zwischen den verschiedenen Codepunkten von DiffServ, IP-Präzedenz und dem „User Priority“-Feld im Ethernet-Header ist in der folgenden Tabelle dargestellt.

IP-Header									**Ethernet-Header**
DiffServ						vs.	IP-Präzedenz		IEEE802.1p
Code-punkt	Vorbelegung (änderbar)		Drop-Level				Belegung (fest)		
	binär (Bitfeld)	Tos-Feld (hex)	high	med	low		binär (Bitfeld)	Tos-Feld (hex)	User Priority (Binär, Bitfeld)
CS7	111000	E0		x		<->	111	E0	111
AF 11	001010	28			x	->	110	C0	110

Tabelle 3-12 Codepunkt-Umsetzung

IP-Header									Ethernet-Header
DiffServ						vs.	IP-Präzedenz		IEEE802.1p
Code-punkt	Vorbelegung (änderbar)		Drop-Level				Belegung (fest)		
	binär (Bitfeld)	Tos-Feld (hex)	high	med	low		binär (Bitfeld)	Tos-Feld (hex)	User Priority (Binär, Bitfeld)
AF 12	001100	30		x		<->	110	C0	110
AF 13	001110	38	x			->	110	C0	110
AF 21	010010	48			x	->	101	A0	101
AF 22	010100	50		x		<->	101	A0	101
AF 23	010110	58	x			->	101	A0	101
AF 31	011010	68			x	->	100	80	100
AF 32	011100	70		x		<->	100	80	100
AF 33	011110	78	x			->	100	80	100
AF 41	100010	88			x	<->	011	60	011
AF 42	100100	90		x		<->	011	60	011
AF 43	100110	98	x			<->	011	60	011
EF	101110	B8				<->	110	C0	110
DE (default)	000000	00					000 001 010	00 20 40	000

Tabelle 3-12 Codepunkt-Umsetzung

Die Spalte „vs.“ verdeutlicht die Zusammenhänge zwischen den beiden Standards DiffServ und IP-Präzedenz. Da DiffServ mehr Varianten bietet, wird bei der Übersetzung von IP-Präzedenz in DiffServ jeweils der Codepunkt fest ausgewählt: z. B. wird aus „100“ IP-Präzedenz der Codepunkt „AF31“. Bei Paketen, die die HiPath 2000 in Richtung LAN verlassen, wird bei aktiviertem IEEE 802.1p die in der letzen Spalte angegebene User Priority eingestellt.

QoS kann nicht nur für PSTN-Partner, sondern auch für die zweite LAN-Schnittstelle aktiviert werden. Für diese Schnittstelle wird das Interface um eine zusätzliche Begrenzung der Datenrate erweitert. Die Funktionsweise der Qualitätsbewertung entspricht dem Verfahren der PSTN-Partner. Die durchschnittliche Datenrate wird in den Konfigurationsdaten eingestellt.

3.7 Statischer und adaptiver Jitter-Buffer

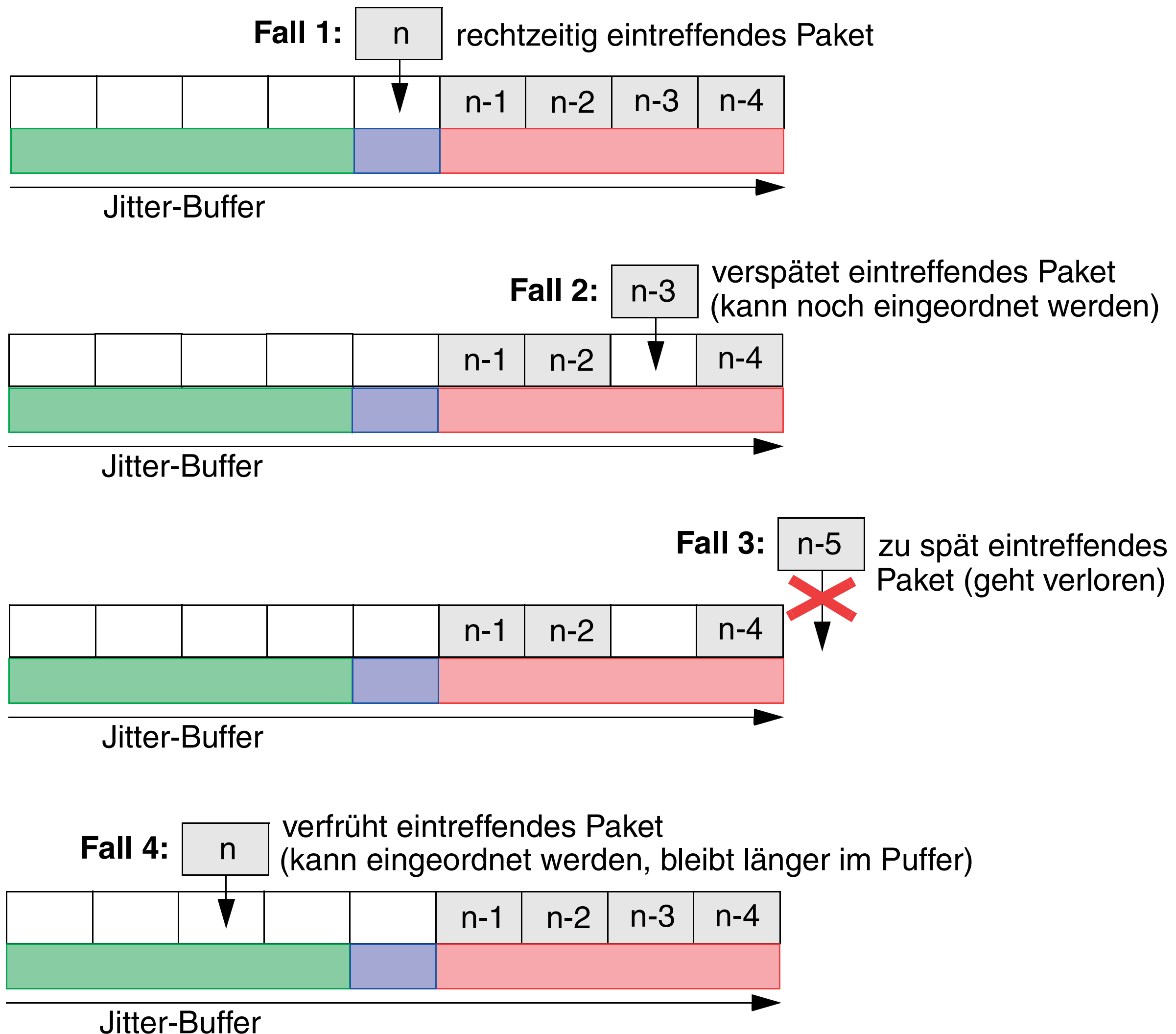
Der Jitter-Buffer der HiPath 2000 kann auf die Verbindungsbedingungen des jeweiligen Netzwerks eingestellt werden.

3.7.1 Funktionalität des Jitter-Buffers

In TCP/IP-basierten Netzwerken können Pakete einer Übertragung unterschiedlich schnell eintreffen. Da sich dieser Effekt vor allem bei Sprachsignalübertragungen störend auswirkt, muss kontrollierend in den Datenstrom eingegriffen werden. Der Jitter-Buffer ist ein Zwischenspeicher für IP-Pakete. Er kann Verzögerungen von IP-Paketen bis zu einem gewissen Grad ausgleichen.

IP-Pakete gelangen in den Jitter-Buffer in der Reihenfolge ihres Eintreffens. Jedes Paket enthält einen Zeitstempel, der im RTP-Header des Pakets gespeichert ist. Aus den Zeitstempeln der Pakete ergibt sich deren tatsächliche Reihenfolge. Der Jitter-Buffer sorgt dafür, dass die Pakete ihn in der tatsächlichen Reihenfolge und zeitlich normal wieder verlassen. Eine Durchschnittszeit (Durchschnitts-Delay) definiert, wie lange Pakete, die zum erwarteten Zeitpunkt eintreffen, im Jitter-Buffer bleiben. Pakete, die später eintreffen als erwartet, bleiben entsprechend kürzer im Jitter-Buffer; Pakete, die früher eintreffen als erwartet, entsprechend länger. Wenn ein Paket so spät eintrifft, dass es nicht mehr eingeordnet werden kann, geht es verloren. Theoretisch können Pakete auch so früh eintreffen, dass sie nicht eingeordnet werden können. Dies ist jedoch in der Praxis kaum der Fall.

Die folgende Illustration verdeutlicht die Arbeitsweise des Jitter-Buffers:



Bei Sprachübertragungen ist es akzeptabel, wenn einzelne Pakete verloren gehen. Dagegen sollte die Verzögerung möglichst niedrig sein, da zu große Verzögerungen das Telefonieren beeinträchtigen.

Bei Datenübertragungen sollten so wenig Pakete wie möglich verloren gehen, um die Integrität der Daten sicher zu stellen. Dagegen spielen Verzögerungen keine so große Rolle.

3.7.2 Arbeitsweisen des Jitter-Buffers

Der Jitter-Buffer bietet drei verschiedene Arbeitsweisen an. Davon sind zwei für Sprachübertragung geeignet, und eine für Datenübertragungen (z. B. transparentes Fax, transparentes Modem oder ISDN-Daten):

- **statischer** Jitter-Buffer für Sprache
- **statischer** Jitter-Buffer für Daten
- **adaptiver** (dynamischer) Jitter-Buffer für Sprache

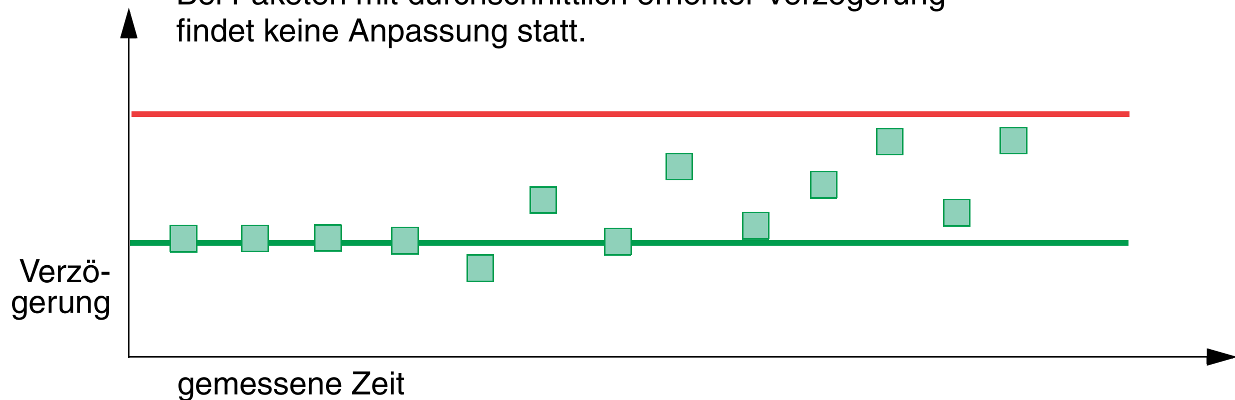
Der adaptive Jitter-Buffer ist speziell für die Sprachübertragung gedacht.Während beim statischen Jitter-Buffer die Durchschnittsverzögerung für Pakete konstant bleibt, wird diese beim adaptiven Jitter-Buffer je nach Situation automatisch angepasst. Die folgende Illustration verdeutlicht den Unterschied zwischen statischem und adaptivem Jitter-Buffer anhand einer Situation, in der vermehrt Pakete mit erhöhter Verzögerung eintreffen:

Legende: rote Linie: maximale Verzögerung (einstellbar)

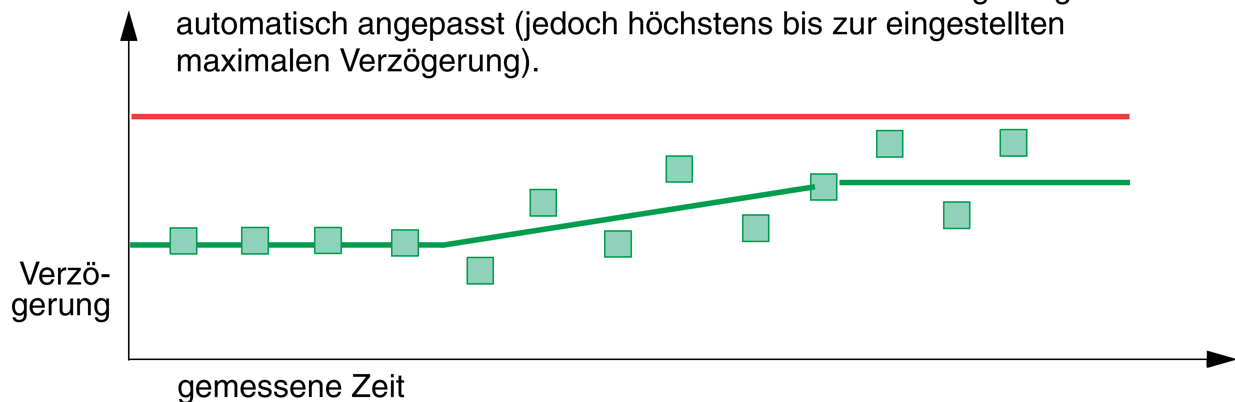
grüne Linie: durchschnittliche Verzögerung (einstellbar, bei akaptivem Jitter-Buffer jedoch nur als Startwert zu verstehen)

Quadrat: Pakete

Statischer Jitter-Buffer: Durchschnittliche Verzögerung ist konstant. Bei Paketen mit durchschnittlich erhöhter Verzögerung findet keine Anpassung statt.



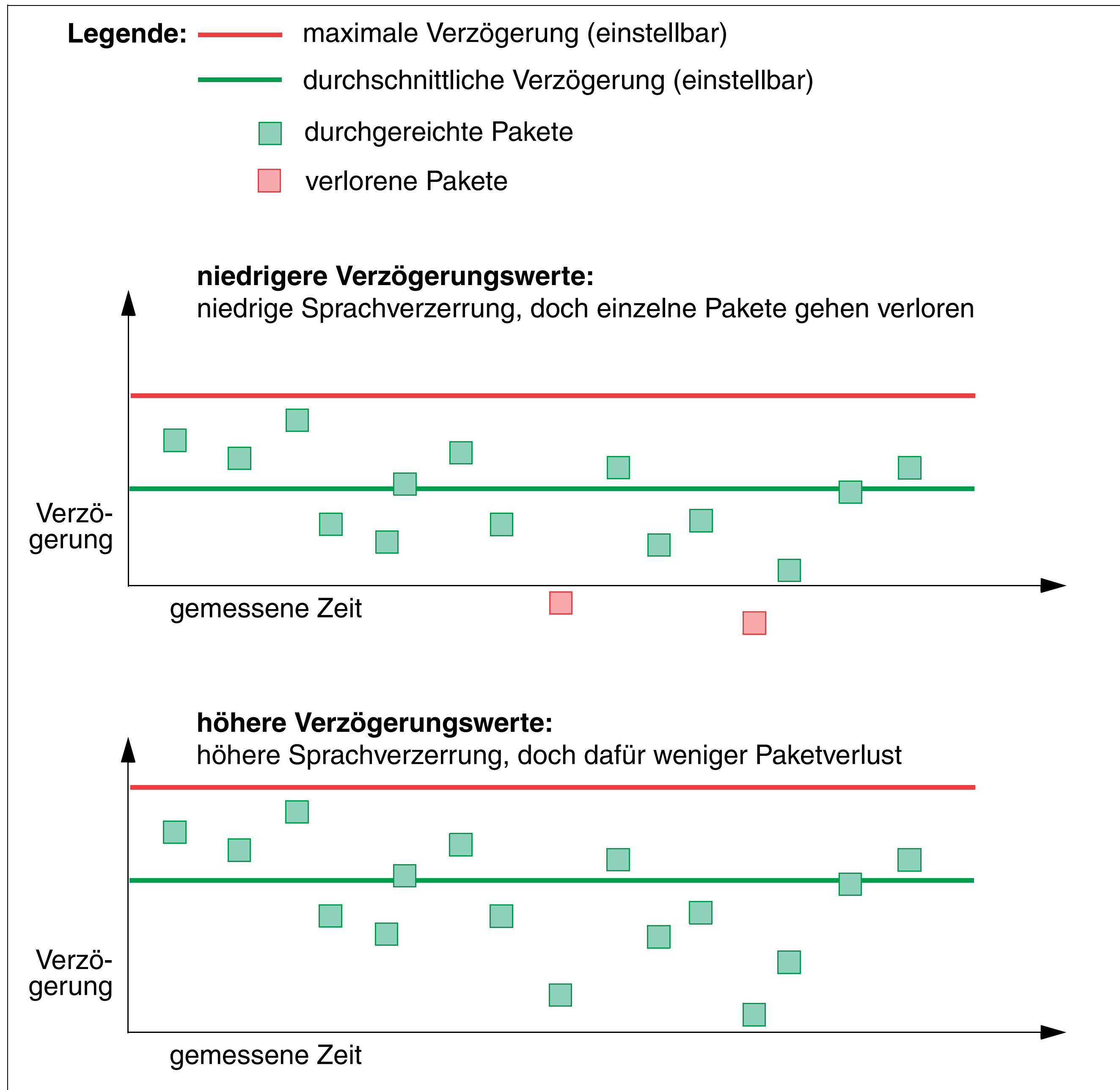
Adaptiver Jitter-Buffer: Durchschnittliche Verzögerung ist variabel und wird bei Paketen mit durchschnittlich erhöhter Verzögerung automatisch angepasst (jedoch höchstens bis zur eingestellten maximalen Verzögerung).



Die einstellbare durchschnittliche Verzögerung (grüne Linie) ist beim adaptiven Jitter-Buffer lediglich der Startwert.

3.7.3 Abwägungen beim Einstellen der Verzögerung bei statischem Jitter-Buffer

Je niedriger durchschnittliche und maximale Verzögerung eingestellt werden, desto verzerrungsfreier ist vor allem die Übertragung von Sprache. Dafür steigt die Gefahr des Paketverlusts. Bei höheren Werten für die Verzögerung können weniger Pakete verloren gehen, doch dafür steigt der Verzerrungsfaktor. Die folgende Illustration verdeutlicht diesen Zusammenhang:

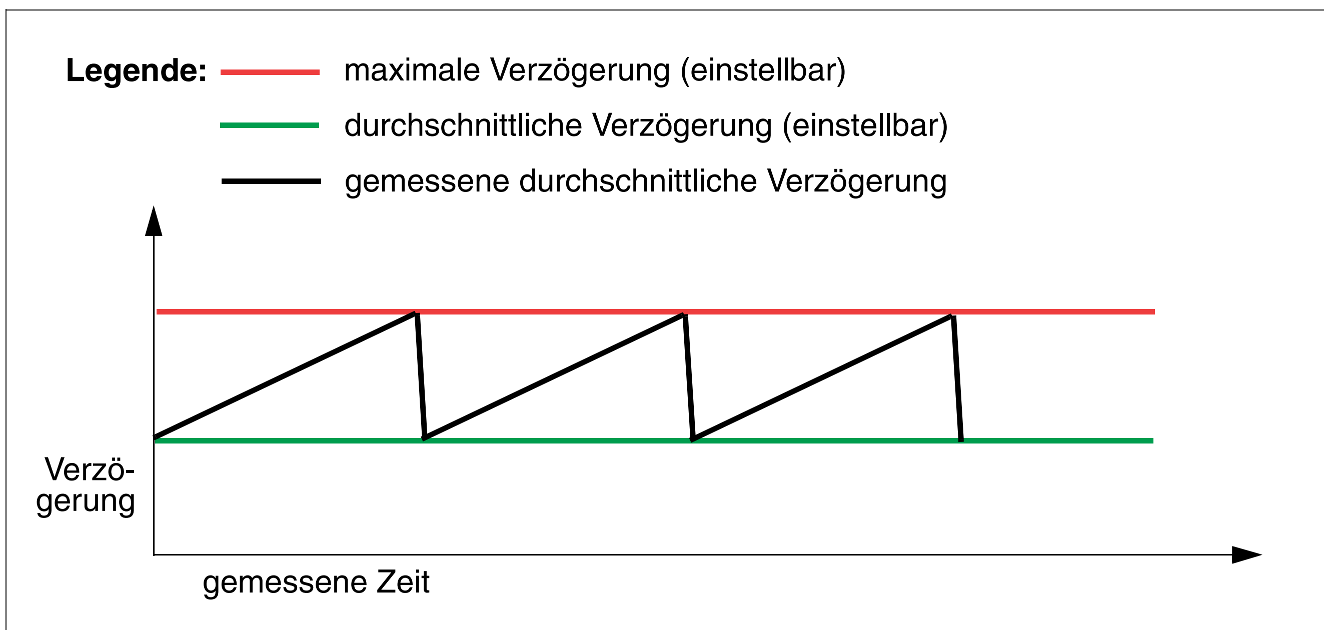


Die HG-Baugruppe ist auf Mittelwerte voreingestellt, die sich in den meisten Umgebungen bewährt haben.

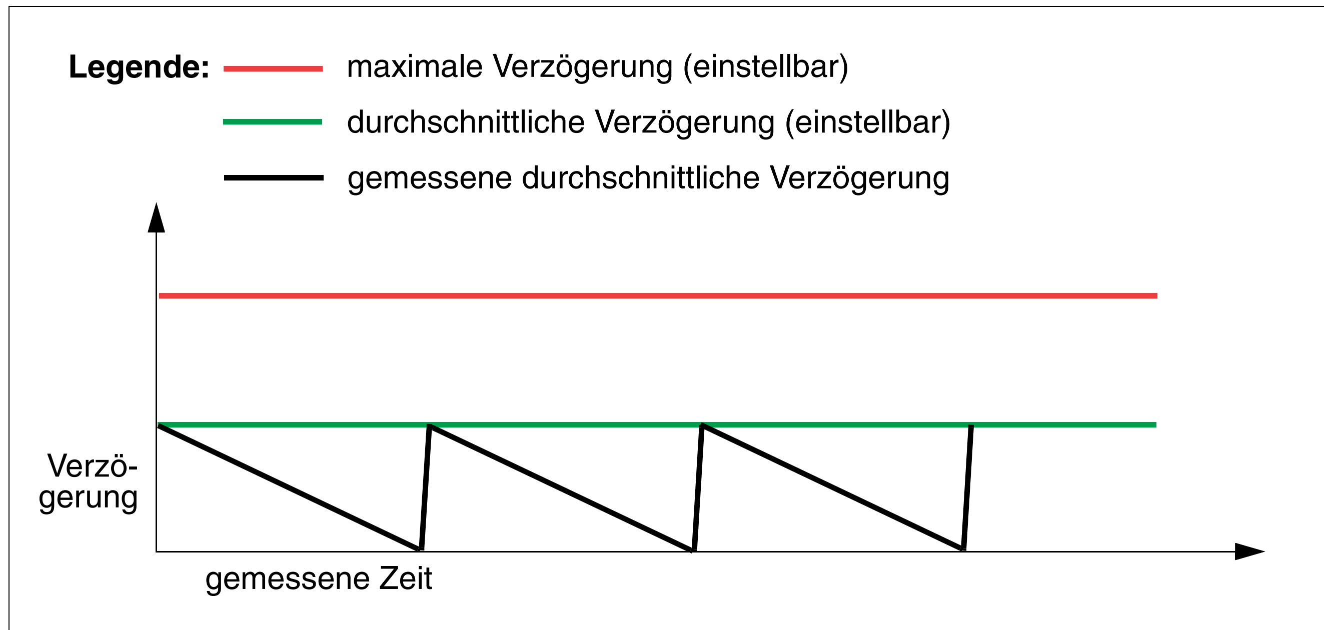
3.7.4 Clock Drift bei statischem Jitter-Buffer

Für die Zeitstempel der Pakete einer IP-basierten Sprachübertragung sorgt gemessene Uhrzeit. Wenn die Zeitmessung auf Sender- und Empfängerseite nicht exakt übereinstimmt, führt dies dazu, dass auf der Sendeseite mehr oder weniger Pakete pro Sekunde erzeugt werden, als auf Empfängerseite erwartet werden. Diese Diskrepanz wird als Clock Drift bezeichnet.

Wenn auf Empfängerseite mehr Pakete erzeugt werden, als im Jitter-Buffer der HG-Baugruppe erwartet werden, gelangen mehr Pakete in den Jitter-Buffer als vorgesehen. Das führt zu einem ständigen Anstieg der gemessenen durchschnittlichen Verzögerung. Wenn diese den eingestellten Maximalwert für Verzögerung erreicht, reguliert sich der Jitter-Buffer. Er überspringt überzählige Pakete, bis die gemessene durchschnittliche Verzögerung wieder den eingestellten Wert für durchschnittliche Verzögerung erreicht. Der gesamte Vorgang beginnt von Neuem. Die folgende Abbildung verdeutlicht den Vorgang:

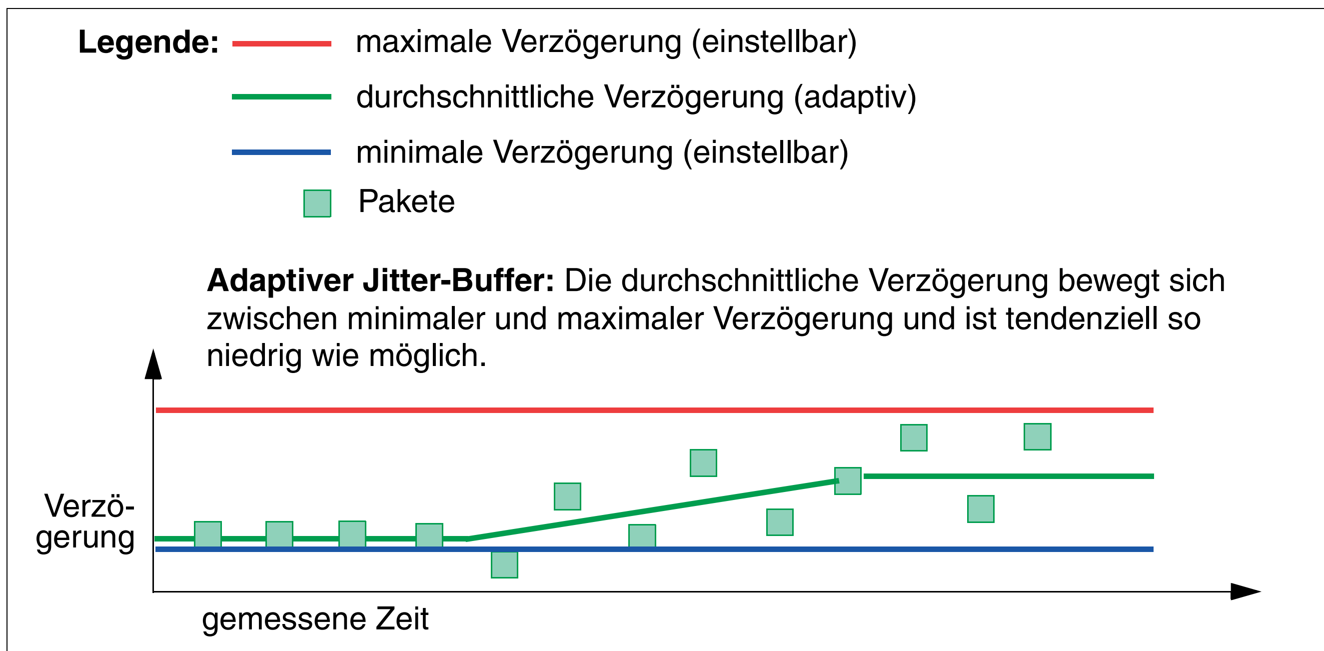


Wenn auf Empfängerseite wenger Pakete erzeugt werden, als im Jitter-Buffer der HG-Baugruppe erwartet werden, gelangen weniger Pakete in den Jitter-Buffer als vorgesehen. Das führt zu einer ständigen Verringerung der gemessenen durchschnittlichen Verzögerung. Wenn dies dazu führt, dass sich gar keine Pakete mehr im Jitter-Buffer befinden, reguliert sich der Jitter-Buffer und passt die gemessene durchschnittliche Verzögerung wieder an den eingestellten Wert für durchschnittliche Verzögerung an. Der gesamte Vorgang beginnt von Neuem. In diesem Fall gehen keine Pakete verloren. Die folgende Abbildung verdeutlicht den Vorgang:



3.7.5 Minimalverzögerung bei adaptivem Jitter-Buffer

Im adaptiven Arbeitsmodus versucht der Jitter-Buffer, die durchschnittliche Verzögerung so gering wie möglich zu halten. In einer Situation, in der kein Jitter-Effekt auftritt, sinkt die durchschnittliche Verzögerung auf ein Minimum. Dieses Minimum ist in der HG-Baugruppe einstellbar. Die durchschnittliche Verzögerung, die auf Basis der aktuell gemessenen Verzögerung laufend angepasst wird, bewegt sich also zwischen zwei Grenzen: der einstellbaren Minimalverzögerung und der einstellbaren Maximalverzögerung. Die folgende Illustration verdeutlicht dies:



3.7.6 Paketverlustkontrolle bei adaptivem Jitter-Buffer

Um zu hohen Paketverlust zu vermeiden, wird die tatsächliche Berechnung der durchschnittlichen Verzögerung beim adaptiven Jitter-Buffer durch zwei Faktoren beeinflusst:
1. durch die laufend gemessene Verzögerung
2. durch die Anzahl verlorener Pakete.

Der Wirkungsgrad des zweiten Faktors ist durch einen „Präferenz“-Parameter in der HG-Baugruppe einstellbar. Mit Werten zwischen 0 und 8 lässt sich einstellen, ob beim Berechnen der durchschnittlichen Verzögerung tendenziell mehr Gewicht auf die Minimierung der Verzögerung oder auf die Vermeidung von Paketverlust gelegt werden soll. Dabei bedeutet 0 „Paketverlust möglichst vermeiden“ und 8 „Durchschnittsverzögerung möglichst gering halten“. Voreingestellt ist ein mittlerer Wert (4).

Als Daumenregel gilt: der Wert 0 wird ca. 10ms höhere Durchschnittsverzögerung bewirken als der mittlere Wert 4, und der Wert 8 ca. 10ms geringere Durchschnittsverzögerung als der mittlere Wert 4.

3.8 SSL und VPN

SSL wird zur gesicherten Datenübertragung zwischen dem Web-Browser des Administrations-PCs und dem Webserver der HiPath 2000 eingesetzt.

SSL stellt folgende Sicherungsdienste zur Verfügung:

- Authentizität (der Kommunikationspartner ist der, der er zu sein vorgibt) ,

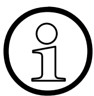
- Vertraulichkeit (die Daten können von einem dritten nicht mitgelesen werden)
- Integrität (die Daten wurden so empfangen wie sie gesendet wurden).

Diese Sicherungsdienste erfordern eine vorherige Verständigung auf einen Sicherheitsmechanismus und den Austausch von kryptographischen Schlüsseln. Diese beiden Aufgaben werden beim Verbindungsaufbau erledigt. Dabei überträgt der Server sein SSL-Zertifikat mit seinem öffentlichen Schlüssel zum Client. SSL nutzt das Public-Key-Verfahren. Auf der Seite des Clients wird ein Master-Schlüssel für die jeweilige SSL-Verbindung erzeugt. Dieser wird, geschützt durch den öffentlichen Schlüssel des Servers, zum Server transportiert. Dann errechnen beide Seiten jeweils auf deterministische Weise (d. h. ohne weiteres Geheimnis) aus diesem Masterkey einen Client-Session-Schlüssel bzw. einen Server-Session-Schlüssel. Der Server-Session-Schlüssel wird für den Weg von Server zu Client verwendet, und der Client-Session-Schlüssel für die Gegenrichtung.

VPN-Funktionen dienen ebenfalls der gesicherten Nutzdatenübertragung mit gewährleisteter Authentizität, Vertraulichkeit und Integrität. Im Gegensatz zu SSL, wo nur TCP-Datenströme gesichert werden, können bei einem VPN, das mit IPSec realisiert ist, alle Daten gesichert werden, die in IP-Paketen übertragen werden, wie TCP- UDP- oder ICMP-Daten.

SSL verwendet **Zertifikate und Schlüssel**, um eine gesicherte Datenübertragung zu ermöglichen. Bei VPN werden Zertifikate (Digitale Signaturen) oder Preshared Keys zur Authentifizierung verwendet. Die Datenübertragung wird mit den während des Schlüsseltausches (ISAKMP/IKE) erzeuten symmetrischen Schlüsseln gesichert. Bei VPN-Verbindungen spricht man von **Tunneln** (siehe Abschnitt 3.8.3, “IPsec-Tunnel”) zwischen den Kommunikationspartnern, die über eine IP-Verbindung telefonieren oder Daten austauschen. Mit Hilfe verschiedener **Dienste** und **Regeln** werden solche Verbindungen konfiguriert.

3.8.1 Verschlüsselung und Schlüssel



Für VPN-Funktionen müssen Sie die erforderliche Lizenz erworben und eingerichtet haben (siehe Abschnitt 1.4, “Lizenzierung”).
Für die Nutzung von SSL sind keine Lizenzen erforderlich.

Schlüssel können folgende Funktionen haben:

- Sicherstellung, dass Daten unverändert und unmanipuliert übertragen werden,
- Unkenntlichmachen von Daten nach außen.

Grundsätzlich wird zwischen symmetrischer und asymmetrischer Verschlüsselung unterschieden. Bei symmetrischer Verschlüsselung wird nur ein Schlüssel benötigt, der zugleich der Verschlüsselung und der Entschlüsselung dient. Sender und Empfänger einer so verschlüsselten Datenübertragung müssen beide in Besitz des Schlüssels sein. Bei der asymmetrischen Verschlüsselung wird zwischen öffentlichem und privatem Schlüssel (**public key** und **private key**) unterschieden. Der öffentliche Schlüssel des Empfängers dient dabei der Verschlüsselung,

und dessen privater Schlüssel der Entschlüsselung. Sender und Empfänger müssen dabei nur den öffentlichen Schlüssel austauschen. Zum Entschlüsseln verwenden sie ihre privaten Schlüssel.

Ein Vorteil der asymmetrischen Verschlüsselung ist also, dass Sender und Empfänger kein Geheimnis (den einzigen Schlüssel) teilen müssen. Stattdessen müssen sie jedoch dem öffentlichen Schlüssel trauen. Die Vertrauenswürdigkeit öffentlicher Schlüssel wird durch **Zertifikate** geregelt.

In der Praxis werden symmetrische und asymmetrische Verschlüsselung häufig gemischt, da asymmetrische Verschlüsselung sehr viel Rechenleistung erfordert. Das Mischen besteht darin, dass ein zeitlich begrenzter Schlüssel (auch **Session-Key** genannt) mit Hilfe symmetrischer Verschlüsselung die eigentlichen Daten ver - und entschlüsselt. Nur der Session-Key selbst wird über asymmetrische Verschlüsselung ausgetauscht.

Zusätzliche Sicherheit verschaffen sogenannte digitale **Signaturen**. Denn die eigentliche Datenverschlüsselung sorgt lediglich dafür, dass „Abhörversuche" nur sinnlosen Datenmüll erhalten. Damit außerdem sichergestellt wird, dass die Daten tatsächlich von dem Sender kommen, von dem sie zu kommen vorgeben, gibt es die Signaturen. Die Signatur ist eine vergleichsweise kurze Zeichenfolge, die aber eindeutig ist. Sie entspricht damit in der Funktion einer persönlichen Unterschrift.

Eine Signatur wird in zwei Schritten erzeugt. Im ersten Schritt wird aus den zu übertragenden Daten eine Art Prüfsumme gebildet. Zur Erzeugung solcher Prüfsummen gibt es spezielle Algorithmen, die sogenannten **Hash-Algorithmen**. Diese erlauben es, aus beliebig langen Bytefolgen eine Bytefolge mit fester Länge zu generieren. Ändert sich nur ein Bit in den Daten, so erzeugen die Hash-Algorithmen eine völlig andere Prüfsumme. Die Prüfsumme wird mit dem privaten Schlüssel des Senders verschlüsselt und kann durch Entschlüsseln mit dem öffentlichen Schlüssel des Senders von jedermann überprüft werden. Dadurch lässt sich die Absenderschaft eindeutig feststellen.

Schlüssel und Prüfsummen werden mit Hilfe von Verschlüsselungsverfahren (Verschlüsselungsalgorithmen) erzeugt. Folgende Verfahren sind im Zusammenhang mit HiPath 2000 von Bedeutung:

- **DES**
  DES steht für Data Encryption Standard. DES ist symmetrische Verschlüsselung gedacht. Die Schlüssellänge beträgt 64 Bit (8 Zeichen).
- **3DES**
  3DES leitet sich von DES ab und steht für Dreifach-Verschlüsselung. Die Schlüssellänge beträgt 192 Bit (24 Zeichen).
- **AES**
  AES steht für Advanced Encryption Standard. AES ist ebenfalls für die symmetrische Verschlüsselung gedacht. Die Schlüssellänge beträgt 128 Bit (16 Zeichen).

- **RSA**
  RSA steht für Rivest Shamir und Adleman. RSA ist ein Algorithmus für asymmetrische Verschlüsselung.
- **MD5**
  MD steht für Message-Digest, die 5 für eine neuere Variante des MD-Algorithmus. MD5 ist ein reiner Hash-Algorithmus und erzeugt aus beliebigen Datenlängen eine eindeutige, 128 Bit (16 Zeichen) umfassende Prüfsumme.
- **SHA1**
  SHA steht für Secure Hash Algorithmus, die 1 für eine neuere Version davon. SHA1 ist ein Hash-Algorithmus und erzeugt aus Datenlängen unter 2^{64} Bit eine Prüfsumme von 160 Bit (10 Zeichen) Länge.

3.8.2 Zertifikate

Zertifikate gewährleisten die Authentizität von öffentlichen Schlüsseln, indem sie den öffentlichen Schlüssel an die Identität des Inhabers binden.

Ein Zertifikat enthält folgende typischen Angaben:

- den Namen des Inhabers,
- den öffentlichen Schlüssel des Inhabers,
- eine Signatur der Zertifizierungsstelle zu Name und Schlüssel,
- Angaben zu den Algorithmen, mit denen die öffentlichen Schlüssel benutzt werden können,
- Beginn und Ende der Gültigkeit des Zertifikats,
- eine Seriennummer,
- den Namen der Zertifizierungsstelle.

Vor einer gesicherten Datenübertragung werden zunächst die Zertifikate von Absender und Empfänger der Daten ausgetauscht und überprüft. Gegebenenfalls werden dann noch Session Keys ausgehandelt. Erst dann werden die Nutzdaten übertragen.

Sender von Daten können ihre Zertifikate selbst erzeugen (selbst signieren). Wenn dies jedoch für die Vertrauenswürdigkeit nicht genügt, sind Zertifikate von Vorteil, die von einer unabhängigen, allgemein bekannten und vertrauenswürdigen Stelle erzeugt (signiert) wurden. Zu diesem Zweck gibt es Zertifizierungsstellen (CAs). Es gibt z. B. öffentliche CAs wie Universitäten, Verlage oder Behörden.

CAs können Hierarchien bilden. So können Zertifikate von CAs selbst wieder von höherinstanzlichen CAs erzeugt worden sein. Das Zertifikat einer Universität könnte beispielsweise von einer staatlichen Zertifizierungsstelle erzeugt worden sein.

Eine Umgebung, in der Zertifikate und deren Eigentümer zentral verwaltet werden, wird als **Public Key Infrastructure (PKI)**.bezeichnet. Zertifikate werden dabei von CAs ausgestellt. Um die Zertifikatsverwaltung zu erleichtern, lässt sich in der HiPath 2000 eine PKI erstellen. Über die PKI lassen sich Server einrichten, auf denen die im VPN konfigurierten Zertifikate und Zertifikatssperrlisten zentral zur Verfügung stehen.

Für die SSL- und VPN-Funktionen in der HiPath 2000 werden je nach Aufgabe unterschiedliche Zertifikate verwendet. Die nachfolgende Aufstellung bietet eine Übersicht über die verwendeten Zertifikate und deren Bezeichnungen.

- **CA-Zertifikat**
  Zertifikat einer Zertifizierungsstelle (CA). Ein CA-Zertifikat kann selbstsigniert oder CA-signiert sein. Bei einem selbstsignierten CA-Zertifikat ist die CA die höchstinstanzliche Vertrauensstelle. Bei einem CA-signierten CA-Zertifikat ist die CA Teil einer CA-Hierarchie.
  In der HiPath 2000 ist das Zertifikat der Lightweight CA bzw. der SSL-Zertifikatsgenerierung ein selbstsigniertes CA-Zertifikat. Das Lightweight CA ist immer eine Stammzertifizierungsstelle (Root CA). Die Funktionalität einer Zwischenzertifizierungsstelle wird nicht unterstützt.
- **Selbstsignierte Zertifikate**
  Bei einem selbstsignierten Zertifikat sind „Subject"und „Issuer" identisch. Es gibt keine höherinstanzliche Vertrauensstelle. Auch CA-Zertifikate können selbstsigniert sein.
- **CA-signierte Zertifikate**
  Solche Zertifikate wurden im Gegensatz zu selbstsignierten Zertifikaten von einer CA signiert. Auch CA-Zertifikate können CA-signiert sein (CA-Hierarchie).
- **Trusted-CA-Zertifikate bzw. Trusted-Zertifikate**
  Wenn ein CA durch Import des CA-Zertifikates vom Nutzer als vertrauenswürdig eingestuft wurde, wird es für diesen Nutzer zum Trusted CA. Die HiPath 2000 akzeptiert bei der VPN-Authentifizierung nur Peer Zertifikate, die von einem Trusted CA herausgegeben wurden.
  In der HiPath 2000 werden im Ordner „Trusted CA-Zertifikate" nur CA-Zertifikate akzeptiert. Im Internet Explorer dagegen können sowohl selbstsignierte als auch CA-signierte Peer- und CA-Zertifikate als Trusted-Zertifikate importiert werden.
- **Serverzertifikat**
  Von einem Serverzertifikat wird dann gesprochen, wenn es sich bei dem Datenaustausch um eine typische Client-Server-Kommunikation handelt, etwa zwischen Browser und Webserver. Mit einem Serverzertifikat weist sich ein Server seinen Clients gegenüber aus und teilt ihnen seinen „Public Key" mit. In der Literatur finden Sie gelegentlich auch den Begriff „User-Zertifikat". Ein Serverzertifikat kann selbstsigniert oder CA-signiert sein.
- **Peer-Zertifikat bzw. VPN-Peer-Zertifikat**
  Anstelle von „Serverzertifikat“ wird im Zusammenhang mit IPsec bevorzugt von „Peer-Zertifikat“ bzw. „VPN-Peer-Zertifikat“ gesprochen. Der Grund besteht darin, dass bei IPsec

beide Kommunikationspartner ein Zertifikat besitzen und es bei der Kommunikation über einen IPsec-Tunnel keine Rollenverteilung in Client und Server gibt. Ein Peer-Zertifikat ist immer CA-signiert.

- **Root-Zertifikat**
  Ein Root-Zertifikat ist das oberste Zertifikat einer PKI. Ein Root-Zertifikat ist immer ein selbst signiertes CA-Zertifikat.

3.8.3 IPsec-Tunnel

IPsec (IP Security) ist ein Internet-Standard, der den Aufbau von sicheren IP-Verbindungen zwischen zwei Endpunkten (Peer-to-peer-Kommunikation) ermöglicht. Dabei wird zwischen den IP-Adressen der Verbindung ein sogenannter IPsec-Tunnel aufgebaut. IPsec-Tunnel werden für VPNs verwendet. Ein IPsec-Tunnel besteht aus folgenden Sicherheitsfunktionen:

- **Paketverschlüsselung**
  Alle IP-Pakete können verschlüsselt übertragen werden. Dazu werden Verschlüsselungsverfahren (Verschlüsselungsalgorithmen) verwendet. Bei der Paketverschlüsselung wird zwischen zwei Arten unterschieden: dem Transportmodus und dem Tunnelmodus. Beim Transportmodus werden nur die Nutzdaten verschlüsselt, im Tunnelmodus sowohl die Nutzdaten als auch die IP-Header-Daten.

- **Paketintegrität**
  IPsec stellt sicher, dass alle IP-Pakete unmanipuliert beim Empfänger ankommen. Dazu werden Hash-Verfahren wie MD5 oder SHA angewendet. Jede Bit-Manipulation im Datenpaket bewirkt nach Anwendung eines Hash-Verfahrens eine völlig neue Bytefolge, so dass selbst Manipulationen auf Bit-Ebene zuverlässig erkannt werden.

- **Paketauthentizität**
  IP-Pakete gelten als „authentisch“, wenn die IP-Adressen von Sender und Empfänger während der Datenübertragung nicht manipulierbar sind, d.h. wenn sicher ist, dass die Daten von dem Empfänger kommen, von dem zu kommen sie vorgeben. Auch hierfür werden Hash-Verfahren eingesetzt.

- **Schlüsselverwaltung**
  Zur Schlüsselverwaltung wird immer der IKE-Dienst verwendet. Zur Schlüsselverwaltung gehört die Art der Verschlüsselung, die verwendeten Schlüssel und deren Gültigkeitsdauer. Alle diese Parameter werden in der sogenannten **Security Association (SA)** beschrieben.

3.8.3.1 VPN-Verbindungen

Die HiPath 2000 unterstützt bis zu 10 Tunnnel.

VPN-Verbindungen mit der HiPath 2000 erfordern immer drei SAs:

- eine für die anfängliche gegenseitige Authentifizierung und für den Austausch der Session-Keys (IKE-SA)
- jeweils eine pro Richtung der eigentlichen aufgebauten Verbindung für den Payload-Verkehr (Payload-SAs)

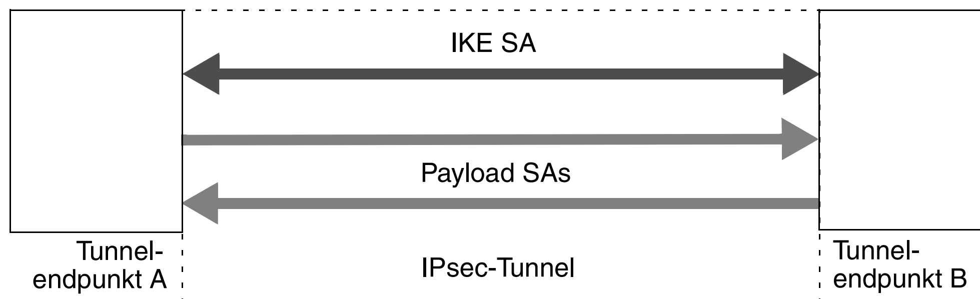


Bild 3-3 Security Association eines VPN-Tunnels

Tunnel müssen immer in beiden VPN-Partnergeräten eingerichtet werden.

HiPath 2000 verwendet den IPSec -Tunnelmodus mit ESP (Encapsulating Security Payload). Bei ESP handelt es sich um ein IPSec-Protokoll, durch das die Paketverschlüsselung, Paketintegrität sowie die Paketauthentizität sichergestellt wird. Die Integritäts- sowie Authentizitätsprüfung erstreckt sich hierbei jedoch nicht auf den IP-Header sondern nur auf die eigentlichen Daten (Payload).

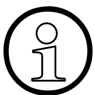
Das IPSec-Protokoll AH (Authentication Header) wird vom HiPath 2000 nicht verwendet. AH stellt die Paketauthentizität und -integrität des gesamten IP-Paketes inklusive Header sicher. Das AH-Verfahren ist insbesondere nicht zusammen mit NAT (Network Address Translation) verwendbar, da durch NAT der IP-Header verändert wird.

3.8.4 Dienste

Für die weiter unten beschriebenen Regeln können optional Dienste definiert werden. In den Regeln kann festgelegt werden, wie mit IP-Paketen eines bestimmten Dienstes zu verfahren ist ("pass", "deny", Verschlüsselung). Ein Dienst wird über Quell-Port, Ziel-Port und IP-Protokoll definiert.

Sie könnten beispielsweise den Dienst HTTP wie folgt definieren:

- Name: HTTP
- Quell-Port: 0 (heißt unbekannt bzw. beliebig)
- Ziel-Port: 80
- IP-Protokoll: TCP



Der Quell- und Ziel-Port 500 kann hierbei nicht konfiguriert werden! Dieser Port wird für das Protokoll IKE (Internet Key Exchange) verwendet. Das IKE-Protokoll regelt in Verbindung mit dem IPSec-Protokoll unter anderem die automatische Auswahl der Verfahren für die Paketverschlüsselung und für die Paketintegrität sowie die Lebensdauer von Schlüsseln.
Für IKE existiert im IPSec-Stack des HiPath 2000 eine bereits vordefinierte, unsichtbare Default-Regel, welche Pakete des IKE-Dienstes immer passieren lässt. Der IKE-Dienst muss nicht konfiguriert werden, da er standardmäßig vorkonfiguriert ist.

3.8.5 Regeln

Regeln sind das übergeordnete Instrument, um aus IPsec-Tunneln und Diensten konkrete VPN-Verbindungen zu konfigurieren.

Eine Regel gibt an, ob auf einem Gateway IP-Pakete zwischen bestimmten festen IP-Adressen oder IP-Adressbereichen über VPN durchgelassen (pass) oder abgewiesen (deny) werden. Dabei sind pass bzw. deny die möglichen **Aktionen** der Regel.

Bei einer Regel mit pass-Aktion wird ferner festgelegt, ob eine Verschlüsselung der Daten erforderlich ist, und welche IPsec-Tunnel und Dienste dazu verwendet werden sollen. Vor dem Einrichten von Regeln müssen daher zuerst IPsec-Tunnel und Dienste eingerichtet worden sein.

Auch die Übertragungsrichtung der IP-Pakete zwischen den IP-Adressen oder IP-Adressbereichen ist von Bedeutung (vergleiche Bild 3-3). Eine Regel wird stets für eine Übertragungsrichtung definiert, es wird also zwischen **Quelladresse** und **Zieladresse** unterschieden. Wird eine Verbindung in dieser Richtung initiiert und laut Regel zugelassen, so wird die Rückrichtung genau dieser Verbindung für eine definierte Zeit automatisch geöffnet. Die Zieladresse kann also der Quelladresse antworten, ohne dass dafür eine Regel notwendig ist. Dies wird durch die

Funktion "Stateful Inspection" des IPSec-Stacks sichergestellt. Für Verbindungen in beide Richtungen, die auch von beiden Seiten initiiert werden können, muss daher nach dem Einrichten einer Regel für eine Richtung stets eine Regel für die Gegenrichtung eingerichtet werden.

Jede Regel verfügt außerdem über eine **Priorität**. Eine Regel für eine Übertragungsrichtung und die dazugehörige Regel für die Gegenrichtung haben stets die gleiche Priorität. Prioritäten werden in Form von frei wählbaren Zahlen vergeben. Höhere Zahlen bedeuten eine niedrigere Priorität, d.h. also die Regel mit Priorität 1 wird zuerst bewertet, da sie die höchste Priorität darstellt.

Eine Regel kann also beispielsweise folgendes definieren:
„IPsec-getunnelte Datenübertragungen vom Host mit der IP-Adresse 192.168.1.50 (Quelladresse) zum Host mit der IP-Adresse 192.168.4.50 (Zieladresse) sollen erlaubt sein. Die Daten müssen verschlüsselt werden. Bei der Quelladresse soll der IPsec-Tunnel mit dem Namen „Tunnel1“ verwendet werden, bei der Zieladresse der IPsec-Tunnel mit dem Namen „Tunnel2. Die Regel soll die Priorität 2 haben.“

Mehrere Regeln enthalten also mehrere Bedingungen. Die Regeln werden nach Priorität abgearbeitet. Die Bedingung der Regel mit der höchsten Priorität wird also zuerst geprüft, und die derjenigen mit der niedrigsten Priorität zuletzt. Sobald innerhalb dieser Abarbeitungsfolge eine Regel gefunden wird, die auf einen konkreten Verbindungswunsch passt, wird diese Regel angewendet. Regeln mit niedriger Priorität, die ebenfalls passen würden, kommen nicht zum Zug. In der Praxis bedeutet das:

- Allgemein gültige Regeln müssen eine niedrigere Priorität haben als einschränkende Regeln. Denn andernfalls würden die allgemeinen Regeln die einschränkenden Regeln „abschatten”, da die Abarbeitung bei der ersten passenden Regel endet.
- Ungenaue bzw. allgemeine Regeln sollten eine niedrigere Priorität haben als genaue Regeln. Eine ungenaue Regel definiert als Quelle oder Ziel ganze Subnetze oder gar die Adresse 0.0.0.0 (=unbekannt). Eine ungenaue Regel mit höherer Priorität "schattet" eine genauer definierte Regel mit niedrigerer Priorität ab, da die Abarbeitung bei der ersten passenden Regel endet.

3.8.6 Authentifizierung

3.8.6.1 Authentifizierung bei SSL

Bei SSL-basierter WBM-Administration findet eine Client-Server-Kommunikation statt.

Der Client, d.h. der Browser, mit dem Sie das WBM starten, authentifiziert sich gegenüber dem Server durch eine Benutzerkennung (Benutzername plus zugehöriges Kennwort). Diese muss zuvor eingerichtet worden sein.

Der Server authentifiziert sich gegenüber dem Client mit Hilfe der durch die SSL-Funktion generierten oder importierten Zertifikate. Im Browser kann ein solches Zertifikat als vertrautes Zertifikat importiert werden, um Warnmeldungen des Browsers beim Verbinden zum SSL-Server (HiPath 2000) zu vermeiden.

3.8.6.2 Authentifizierung bei VPN

Bei VPN findet eine Peer-to-peer-Kommunikation statt. Die Authentifizierung von VPN-Partnern ist auf zwei Arten möglich:

- **Pre-shared Keys**
  Die Authentifizierung durch den gegenüberliegenden Tunnelendpunkt erfolgt über einen sogenannten „Pre-shared Key". Dies ist ein Schlüssel, der bei der Tunnelkonfiguration festgelegt wird. Damit sich die über den Tunnel kommunizierenden VPN-Partner authentifizieren können, muss für beide Tunnelendpunkte das gleiche Kennwort verwendet werden.
- **Digitale Signaturen**
  Jedem VPN-Partner ist ein Zertifikat zugeordnet. Für eine erfolgreiche Authentifizierung müssen die VPN-Partner an beiden Tunnelendpunkten die digitale Signatur des jeweils gegenüberliegenden Partners gegen eine vertrauenswürdige CA prüfen.

3.8.7 SSL und VPN

SSL dient der gesicherten Administration, VPN der gesicherten Nutzdatenübertragung. Insgesamt werden folgende Sicherheitsstufen unterschieden:

- **Gesicherte Administration (Werkszustand)**
  Dies ist der Zustand nach Erstellung des ersten Server-Zertifikats und dem darauf folgenden Einschalten der SSL-Funktion über den CLI-Befehl `enable ssl`. Die Baugruppe kann nun über die Zugänge V.24 (CLI) und HTTPS (WBM) administriert werden. Ungesicherte Zugangsmöglichkeiten (wie Telnet) oder Protokolle (wie z. B. FTP, TFTP) sind gesperrt. Eine IPsec-Policy kann eingerichtet bzw. bearbeitet werden, ist in diesem Zustand aber nicht aktiviert. Somit ist ungesicherter Nutzdatenverkehr möglich.

- **Gesicherter Betrieb**
  Dies ist der Zustand nach Einrichtung und Einschalten der IPsec-Policy. Die Baugruppe befindet sich im gleichen Zustand wie bei der gesicherten Administration. Zusätzlich ist der gesicherte Datenverkehr entsprechend der eingerichteten Security Policy aktiviert.

3.9 H.235 Security

H.235 ist ein Ergänzungsprotokoll, welches das H.323-Protokoll (und andere) um Sicherheitsfunktionen zur Authentifizierung, Datenschutz und Datenintegrität erweitert. H.235 unterstützt verschiedene Verschlüsselungsalgorithmen und einstellbare Optionen wie z. B. die Länge von Schlüsseln.

HiPath 2000 unterstützt das H.235-Protokoll. Die Grundeinstellungen dazu gehören jedoch nicht zum Konfigurationsumfang des Gateways, sondern werden im HiPath 3000 Manager E vorgenommen.

4 Serviceability und Administration

4.1 Übersicht

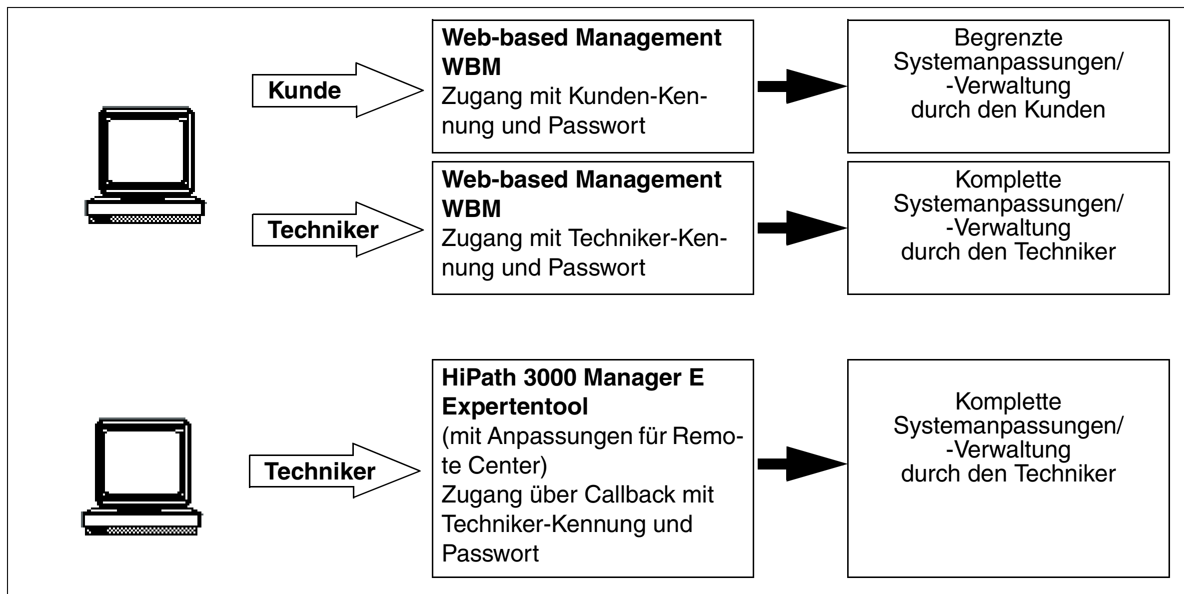
Beschrieben sind die in der folgenden Tabelle genannten Themen.

Thema
Möglichkeiten im Service, Seite 4-2 ● Kundendaten sichern (Backup), Seite 4-3 ● Kundendaten wiederherstellen (Restore), Seite 4-3 ● EVM-Mediendaten sichern (EVM-Backup) (nur für HiPath 2030), Seite 4-4 ● EVM-Mediendaten wiederherstellen (EVM-Restore) (nur für HiPath 2030), Seite 4-4 ● EVM hochrüsten (EVM-Upgrade) (nur für HiPath 2030), Seite 4-4 ● Integrierte Voice Mail-Mailboxen initialisieren (nur für HiPath 2030), Seite 4-5 ● Systemsoftware aktualisieren, Seite 4-5 ● Systeminformationen und SW-Komponenten ermitteln (HiPath Inventory Manager), Seite 4-6 ● Systemkomponenten sichern, Seite 4-6 ● SW-Images für die Software-Hochrüstung von IP-Workpoints, Seite 4-6
Diagnosemöglichkeiten, Seite 4-7 ● Status des Systems ermitteln, Seite 4-7 ● Status der HiPath 2000-Leitungen ermitteln, Seite 4-7 ● Status der Teilnehmer ermitteln, Seite 4-7 ● Workpoints testen, Workpoints testen, Seite 4-8
USB-Schnittstelle, Seite 4-14

4.2 Möglichkeiten im Service

4.2.1 Möglichkeiten der Systemadministration

Übersicht



4.2.2 Kundendaten sichern (Backup)

Hierbei wird unterschieden zwischen

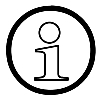
- der Sicherung der Kundendaten **ohne** HiPath Software Manager und
- der Sicherung der Kundendaten **mit** HiPath Software Manager.

4.2.2.1 Kundendatensicherung ohne HiPath Software Manager

Hierunter versteht man das Sichern der kundenindividuellen Daten. Die Sicherung der kundenindividuellen Daten ist möglich mittels:

- HiPath 3000 Manager E
- Web-based Management WBM

4.2.2.2 Kundendatensicherung mit HiPath Software Manager



Der HiPath Software Manager ist nicht Bestandteil der HiPath 2000. Das Tool steht ausschließlich in einem HiPath 3000/HiPath 5000-Netzverbund (ab V6.0) zur Verfügung, in dem auch HiPath 2000 eingebunden ist.

Der HiPath Software Manager ermöglicht Ihnen unter anderem die Sicherung der Kundendatenspeicher aller im gleichen Kundennetz befindlichen HiPath 2000-Systeme, HiPath 3000-Systeme (ab V6.0) und HiPath 5000-Systeme (ab V6.0).

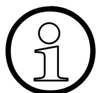
Die KDS-Sicherungen werden in einem vorher zu bestimmenden Verzeichnis abgelegt. Dabei können Sie die Datensicherung entweder sofort manuell starten oder zu einer vorgewählten Zeit durchführen. Ebenso möglich ist eine zyklische Sicherung, die die Kundendaten täglich zu einer definierbaren Zeit speichert.

4.2.3 Kundendaten wiederherstellen (Restore)

Um beschädigte Kundendaten wiederherzustellen, muss ein vorhandenes Backup in das System geladen werden. Die Wiederherstellung der Kundendaten ist möglich mittels:

- HiPath 3000 Manager E
- Web-based Management WBM

4.2.4 EVM-Mediendaten sichern (EVM-Backup) (nur für HiPath 2030)


Während der Sicherung der Mediendaten ist die EVM für den Anwender nicht mehr erreichbar.

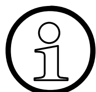
Unter EVM-Backup versteht man das Sichern der kundenindividuellen Ansagen, Begrüßungen und Sprachnachrichten der integrierten Entry Voice Mail EVM.

Ein HiPath 2030-internes automatisches Backup wird über das WBM skaliert (zum Beispiel die Auswahl der Mailboxen). Das aktuelle Backup überschreibt das alte Backup, das heißt in HiPath 2030 ist nur ein Backup (.tar-Datei) vorhanden.

Die manuelle Sicherung der EVM-Mediendaten ist möglich mittels:

- HiPath 3000 Manager E
- Web-based Management WBM

4.2.5 EVM-Mediendaten wiederherstellen (EVM-Restore) (nur für HiPath 2030)

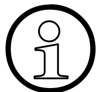

Während der Wiederherstellung der Mediendaten ist die EVM für den Anwender nicht mehr erreichbar.

Durch ein EVM-Restore können Sie gespeicherte Mediendaten (Ansagen, Begrüßungen und Sprachnachrichten) in die EVM der HiPath 2030 laden.

Ein EVM-Restore ist möglich mittels:

- HiPath 3000 Manager E
- Web-based Management WBM

4.2.6 EVM hochrüsten (EVM-Upgrade) (nur für HiPath 2030)


Während einer Hochrüstung ist die EVM für den Anwender nicht mehr erreichbar.

Diese Funktion ermöglicht Ihnen das Laden oder Löschen einer Sprachdatei sowie ein Firmware-Update der EVM. Ein EVM-Upgrade ist möglich mittels HiPath 3000 Manager E.

4.2.7 Integrierte Voice Mail-Mailboxen initialisieren (nur für HiPath 2030)

Das Initialisieren der Integrierte Voice Mail-Mailboxen ist möglich mittels:

- HiPath 3000 Manager E
- Web-based Management WBM

In Abhängigkeit von der Art der Mailbox (Standard oder AutoAttendant Mailboxen) können Sie unter anderem folgende Aktionen durchführen:

- Passwort zurücksetzen
- Nachrichten löschen
- Begrüßungen löschen
- Kurzwahlziele löschen
- manuelle Begrüßungskontrolle einstellen
- Aktive Begrüßung = Begrüßung 1

4.2.8 Systemsoftware aktualisieren

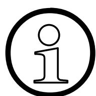
Hierbei wird unterschieden zwischen

- der Aktualisierung der Systemsoftware **ohne** HiPath Software Manager und
- der Aktualisierung der Systemsoftware **mit** HiPath Software Manager.

4.2.8.1 Aktualisierung der Systemsoftware ohne HiPath Software Manager

Die Aktualisierung des Software-Images wird über das Web-based Management WBM durchgeführt.

4.2.8.2 Aktualisierung der Systemsoftware mit HiPath Software Manager



Der HiPath Software Manager ist nicht Bestandteil der HiPath 2000. Das Tool steht ausschließlich in einem HiPath 3000/HiPath 5000-Netzverbund (ab V6.0) zur Verfügung, in dem auch HiPath 2000 eingebunden ist.

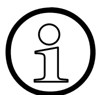
Der HiPath Software Manager ermöglicht unter anderem die Aktualisierung der Systemsoftware (Upgrade Manager) aller im gleichen Kundennetz befindlichen HiPath 2000-Systeme, HiPath 3000-Systeme (ab V6.0) und HiPath 5000-Systeme (ab V6.0).

4.2.8.3 Aktuelle Version der Systemsoftware ermitteln

Die Ermittlung der aktuellen Softwareversionen ist möglich über:

- Web-based Management WBM
  Angezeigt wird unter anderem
  - das aktuelle Gateway-Software-Image
  - ein zur Installation bereitstehendes Gateway-Software-Image
  - die aktuelle HiPath Systemversion
- HiPath 3000 Manager E
  Angezeigt wird ausschließlich die aktuelle Version der Software für das Kommunikationssystem und der Software für das Gateway (Applikations (APP)-File).
- den ersten System Client (nicht optiClient 130)
  Angezeigt wird ausschließlich die aktuelle Version der Software für das Kommunikationssystem und der Software für das Gateway (Applikations (APP)-File).

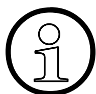
4.2.9 Systeminformationen und SW-Komponenten ermitteln (HiPath Inventory Manager)



Der HiPath Inventory Manager ist nicht Bestandteil der HiPath 2000. Dieser Dienst steht ausschließlich in einem HiPath 3000/HiPath 5000-Netzverbund (ab V6.0) zur Verfügung, in dem auch HiPath 2000 eingebunden ist.

Der HiPath Inventory Manager ist ein Dienst zur Ermittlung der installierten Software-Komponenten und Systeminformationen in einer HiPath-Vernetzung.

4.2.10 Systemkomponenten sichern



Der HiPath Software Manager ist nicht Bestandteil der HiPath 2000. Das Tool steht ausschließlich in einem HiPath 3000/HiPath 5000-Netzverbund (ab V6.0) zur Verfügung, in dem auch HiPath 2000 eingebunden ist.

Der HiPath Software Manager ermöglicht die Sicherung aller HiPath 2000 ComScendo Services in einer HiPath-Vernetzung.

4.2.11 SW-Images für die Software-Hochrüstung von IP-Workpoints

Insgesamt stehen im System 16 MB Speicher für SW-Images zur Verfügung. Dadurch können bis zu fünf SW-Images für die Software-Hochrüstung von IP-Workpoints gleichzeitig bereitgehalten werden.

4.3 Diagnosemöglichkeiten

4.3.1 Status des Systems ermitteln

In der Frontblende des Systems befindet sich die Run-LED, die den aktuellen Status des Systems anzeigt.

4.3.2 Status der HiPath 2000-Leitungen ermitteln

Der aktuelle Status jeder einzelnen Leitung wird von HiPath 2000 in einer Tabelle protokolliert. Bei einem Zustandwechsel wird der neue Status zusammen mit einem Zeitstempel eingetragen.

Die Abfrage des Leitungszustands (Trunk Status) ist mit HiPath 3000 Manager E möglich, wobei folgende Informationen geliefert werden.

Daten	Inhalt
Datum	Datum der Trunk-Status-Abfrage.
Uhrzeit	Uhrzeit der Trunk-Status-Abfrage.
Slot/Port	Slot/Port, an dem die Leitung angeschlossen ist.
Trunk Number	Rufnummer der Leitung (Leitungskennzahl)
Kommentar	Zustand der jeweiligen Leitung

4.3.3 Status der Teilnehmer ermitteln

Der aktuelle Status jedes einzelnen Teilnehmers wird von HiPath 2000 in einer Tabelle protokolliert. Die Abfrage des Teilnehmerzustands ist mit HiPath 3000 Manager E möglich, wobei folgende Informationen geliefert werden.

Daten	Inhalt
Teilnehmername	Name des ausgewählten Teilnehmers
Slot, Port	Slot/Port, an dem der Teilnehmer angeschlossen ist.
Endgerätetyp	zum Beispiel optiPoint 420 advance
Endgerätestatus	aktiv oder inaktiv
Durchwahlnummer	externe Rufnummer des ausgewählten Teilnehmers
Sprache	Menüsprache des ausgewählten Teilnehmers

Daten	Inhalt
Verbindungsstatus	• Inaktiv: Das EG ist frei. • Belegt: Das EG hat eine Belegung gemacht (off hook), aber noch nicht gewählt. • Warten: Der Aufruf des Endgerätes ist in einer Warteschlange. • Verbunden: Das EG steht in einer Verbindung mit einem zweiten EG, mit einer Leitung (Amt) oder mit einem Sammelanschluss-Mitglied. • Halten: Das Endgerät wird gehalten. • Fehler: Die Verbindung kann wegen eines Fehlers nicht aufgebaut werden (zum Beispiel Rufnummer ungültig). • Ruf: Das EG wird gerufen.
Verbunden mit	Rufnummer des verbundenen Teilnehmers oder der Leitung
Weiterleitungsstatus	• Aus: Keine Rufweiterleitung aktiviert. • Intern: Rufweiterleitung nur für interne Gespräche aktiviert. • Extern: Rufweiterleitung nur für externe Gespräche aktiviert. • Alle: Rufweiterleitung für alle Gespräche aktiviert.
Ziel	Rufnummer des Rufweiterleitungsziels
aktivierte Leistungsmerkmale	Zustand der aktivierten Leistungsmerkmale (ein/aus)
Zugeschaltete Teilnehmer	Liste der zugeschalteten Teilnehmer

4.3.4 Workpoints testen

Nach Inbetriebnahme und Länderanpassung kann an jedem optiPoint 600 office, optiPoint 410- und optiPoint 420-Telefon der Endgerätetest über eine Kennzahl oder das Service-Menü aktiviert werden.

Nicht möglich ist der Endgerätetest an optiPoint 600 office S, optiPoint 410 S- und optiPoint 420 S-Telefonen.

Geprüft werden Display (eigene Rufnummer wird angezeigt), LED‘s und Rufe. Der Test beendet sich selbsttätig nach Zeit. Der Tester kann sich während des Tests visuell und akustisch von der Funktion der Komponenten überzeugen.

4.3.5 SNMP benutzen

HiPath 2000 bietet SNMP-Unterstützung an.

Die Applikation zur Nutzung der SNMP-Funktionalität ist ein MIB-Browser, zum Beispiel als Bestandteil des „Network Node Managers“ von Hewlett-Packard.

4.3.5.1 SNMP-Funktionen

Die SNMP-Funktionen umfassen:

- mit MIB-Browser und Standard-MIB (nach RFC1213):
  - Abfragen und Verändern von Standardparametern der MIB 2
- mit MIB-Browser und Private-MIB:
  - Abfragen und Verändern von Parametern der Private MIB der HiPath 2000
- mit HiPath 3000 Manager E:
  - Festlegen von Communities zu Standard-Parametern (Berechtigungsklassen)
  - Festlegen von Trap-Communities und Stationen, an die Traps gesendet werden
  - Festlegen der Traplevel für verschiedene Trapgruppen (Empfindlichkeit auf Fehler)
- mit Trap-Empfänger:
  - Empfangen von Traps

Die MIBs beinhalten für jeden Parameter auch einen Kommentar, der kurz die Bedeutung beschreibt.

Einige Parameter sind hier beispielhaft aufgeführt:

- mgmt > mib-2 > system > sysUpTime: Zeit seit dem letzten Hochlauf der HiPath 2000
- HLB2MIB > siemensUnits > pn > hlb2mib > controlGrouphlb20 > sysSoftwareVersion: SW-Release der Baugruppe
- mgmt->mib-2->ip->ipRouteTable: Routing-Tabelle der HiPath 2000

Die HiPath 2000 sendet SNMP-Traps (Diagnose und Fehlermeldungen) an die unter „SNMP > Trap-Communities“ eingerichteten Stationen. Diese Meldungen werden in Abhängigkeit von den unter „SNMP“ eingestellten Severity-Stufen verschickt.

Beispiele für von der HiPath 2000 generierte Traps:

1. Generische Traps, nicht abschaltbar:
   - warm start
   - cold start
   - authentication failure
2. Enterprise Traps, konfigurierbar
   - data init (WARNING – erzwungene Neuinitialisierung von Daten)
   - memory low (WARNING – Speicherressourcen unterschreiten Schwellwert)

- duplicate mac (MINOR – doppelt vorhandene MAC-Adresse)
- ip firewall (WARNING – IP Firewall Verletzung)
- mac firewall (WARNING – MAC Firewall Verletzung)
- isdn access (WARNING – ISDN Zugangskontrolle)

SNMP-Informationen können auch als E-Mails an eine über WBM konfigurierbare Mailadresse gesendet werden.

4.3.6 Fehlererkennung durch Traps, Traces und Events

Es gibt folgende Möglichkeiten, Fehler der Baugruppe zu erkennen und zu verfolgen:

- **Traps**
  zeigen irreguläre Zustände, kritische Fehler oder wichtige Systeminformationen an.
- **Traces**
  protokolliert die Ausführung einer Softwarekomponente.
- **Ereignisse (Events)**
  melden Systemprobleme oder Systeminformationen.

Traces und Ereignisse werden in jeweils eigene Ereignisprotokolldateien geschrieben.

4.3.6.1 Traps

Bei Problemen in der Baugruppe werden Traps erzeugt, um den Administrator über Fehler zu informieren. Es gibt folgende Arten von Traps:

- System-Traps
- Leistungs-Traps

Die Darstellung der Traps im WBM ist dynamisch. Alle 30 Sekunden wird die Liste der Traps aufgefrischt. Zusätzlich können Sie die Darstellung manuell aktualisieren.

System-Traps

Diese Traps:

- zeigen Systemfehler an und erfordern Gegenmaßnahmen des Administrators,
- oder geben wichtige Systeminformation weiter.

Trap	Empfohlene Maßnahme
Baugruppe wurde erfolgreich gestartet	Nur zur Information, keine Maßnahme erforderlich
Neustart ausgelöst von Administrator, Speicherbereinigung, VxWorks, H.323 oder H.323 Stack Adapter (HSA)	Der Neustart wird ausgeführt, keine Maßnahme erforderlich
Speicherprobleme (Speicher voll, Speicherzuweisung schlug fehl, Speicher ist inkonsistent)	Neustart wird automatisch durchgeführt, keine Maßnahme erforderlich
Internes Softwareproblem (Überprüfung schlug fehl, „Exit“-Ereignis, Problem bei der Konfiguration der Poolgröße, Einrichten einer Sitzung schlug fehl)	Neustart wird automatisch durchgeführt, keine Maßnahme erforderlich
Kapazität des Flash-Speichers ist erreicht	Entfernen Sie nicht benötigte Dateien aus dem Flash-Speicher (sollte nur von einem Systemspezialisten durchgeführt werden)
Ressourcen des IP-Netzstacks sind ausgeschöpft	Überprüfen Sie die IP-Konfiguration des Gateways und der Router
Fehler der SCN-Verbindung (Siemens Corporate Network SCN ausschließlich in Deutschland verfügbar)	Nur zur Information, keine Maßnahme erforderlich

Tabelle 4-1 System-Traps

Leistungs-Traps

Diese Traps zeigen Leistungsprobleme an.

Trap	Empfohlene Maßnahme
Systemspeicher ist voll	keine
DMA-Speicher ist voll	keine

Tabelle 4-2 Leistungs-Traps

4.3.6.2 Traces

Ein Trace protokolliert eine Ausführung einer Softwarekomponente. Ein Fachmann kann mit Hilfe dieser Ablaufaufzeichnung die Ursache eines Fehlers finden.

Die Trace-Ergebnisse können:

- in einer Protokolldatei gespeichert werden und/oder

- über eine LAN-Verbindung direkt auf einen PC gespeichert werden.

Folgende Trace-Funktionen stehen Ihnen zur Verfügung:

Trace-Funktion	Beschreibung
Trace-Format-Konfiguration	Zur Definition der Formate (Header-Daten, Trace-Daten), in der Traces protokolliert werden.
Trace-Ausgabe-Interfaces	Zur Definition der Interfaces, über die die Trace-Ausgabe erfolgen soll.
Trace-Protokoll	Zum Laden der Trace-Protokolldatei von der HiPath 2000 auf den Administrations-PC oder einen anderen Rechner. Ferner kann die Protokolldatei gelöscht werden.
Kunden-Trace-Protokoll	Zur Anzeige der Trace-Historie, das heißt der letzten 50 Ereignisse (Trace-Meldungen).
Trace-Profile	Zur Definition, welche Daten in welcher Detailtiefe protokolliert werden sollen. Es können individuelle Trace-Profile angelegt, geändert und gelösscht werden. Darüber hinaus stehen vordefinierte Trace-Profile zur Verfügung.
Trace-Komponenten	Zur Definition der System-Komponenten, für die Prozess- und Zustandsinformationen protokolliert werden sollen

Tabelle 4-3 Trace-Funktionen

4.3.6.3 Ereignisse (Events)

Ereignisse (Events) informieren Sie über Mängel des Systems. Sie sollten die Konfiguration des Netzwerks und/oder des Gateways überprüfen, um die abnormale Situation zu bereinigen.

Abhängig von der Einstellung und der Problemklasse können Ereignisse einen SNMP-Trap erzeugen, eine E-Mail auslösen, eine Trace-Überwachung starten und/oder einen Reboot des Systems auslösen.

Alle Ereignisse werden in eine Protokolldatei beschränkter Größe geschrieben. Wenn die maximale Größe der Datei überschritten wird, überschreiben neue Meldungen die ältesten Einträge.

Der Name der Ereignisprotokolldatei ist:

`evtlog.txt`

Sie ist in folgendem Verzeichnis im Flash-Speicher der HiPath 2000 gespeichert:

`\tffs\evtlog`

Das Ereignisprotokoll kann auf einen PC übertragen werden. Verwenden Sie dazu die Wartungsfunktion „Laden über HTTPS“ des WBM.

Die einzelnen Einträge haben folgende Bedeutungen:

Eintrag in der Protokolldatei	Bedeutung
IFTABLE	Name der Komponente, die das Ereignis ausgelöst hat
tH323-CLP	Name der Task, die das Ereignis ausgelöst hat
03/17/2000	Datum des Ereignisses
08:13:56.828020	Zeitpunkt des Ereignisses in hh:mm:ss (Sekunden mit sechs Nachkommastellen)
ciftable01.cpp 433	Name der Quelldatei und Nummer der Zeile, bei der das Ereignis auftrat
csevWarning	Ereignisklasse
MSG_DVMGR_INTERROR_DEVID	Interner Code des Ereignisses
DeviceID(0XFFFFFFFF): CIIfTable:: fCheckConsistency Persistency files and hw_specification inconsistent!	Text in der Ereignisdatei

Tabelle 4-4 Bedeutungen von Einträgen in der Ereignisprotokolldatei

4.4 USB-Schnittstelle

HiPath 2020 und HiPath 2030 sind mit jeweils einer USB-Schnittstelle (USB V1.1, Slave Mode) ausgestattet. Die Nutzung ist ausschließlich für Servicezwecke freigegeben.



Bild 4-1 HiPath 2020 und HiPath 2030 (dargestellt) – USB-Anschluss

Nicht für USA: USB-Anschlusskabel

Das USB-Anschlusskabel C39195-Z7702-A20 gehört zum Lieferumfang.

5 Middleware

5.1 HiPath TAPI 120 V2.0

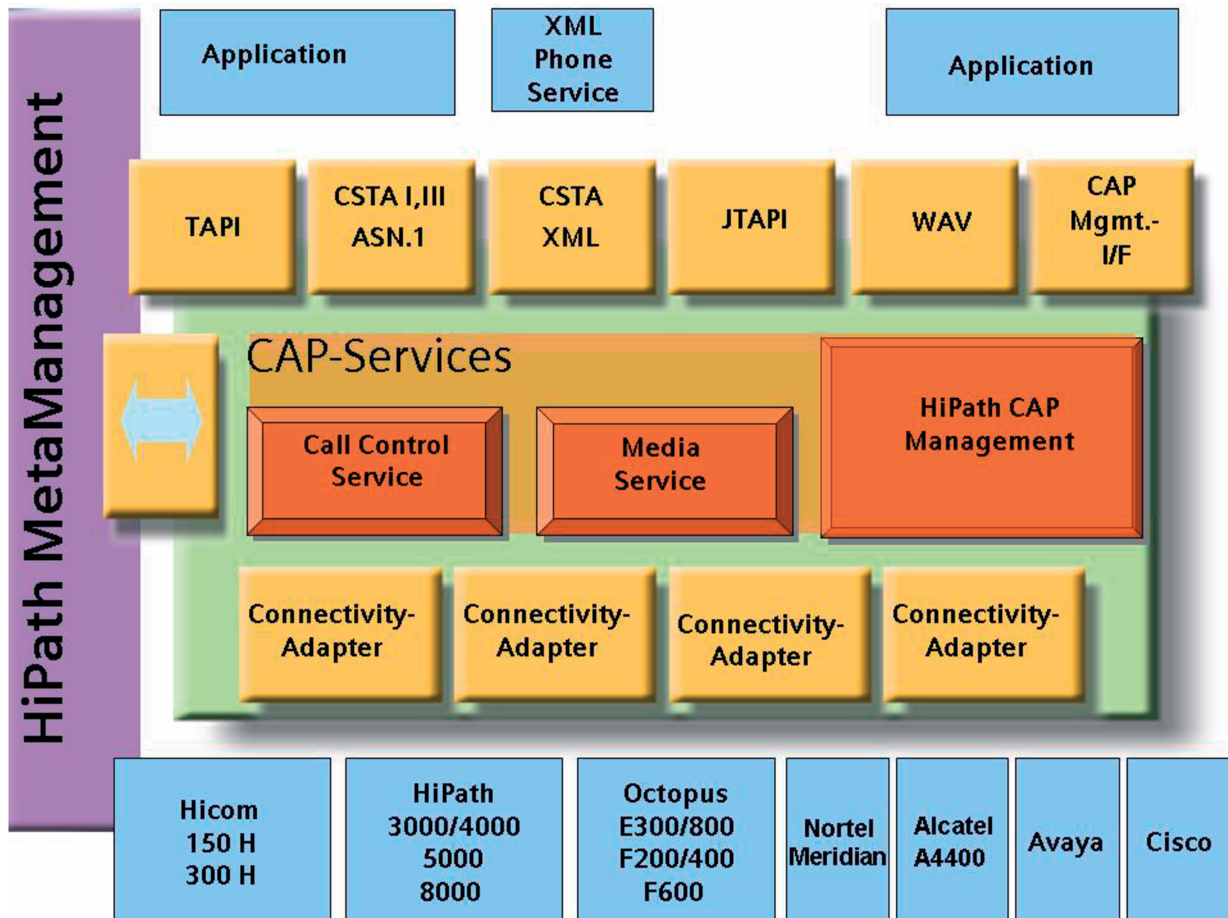
Die 1st party CTI-Funktionalität steht bei allen Modellen der HiPath 2000 zur Verfügung. Bis zu sechs TAPI 120 können lizenzfrei betrieben werden. Zusätzlich zu installierende TAPI 120 sind lizenzpflichtig. Die Software, Installationsanleitung und ergänzende Informationen (Datenblatt) sind im Internet unter http://www.siemens.de/enterprise erhältlich.

5.2 HiPath CAP 3.0

HiPath CAP ist eine leistungsfähige Middleware, die modular skalierbar ist. Sie unterstützt effiziente Verbesserungen und ermöglicht eine Kostenreduzierung durch:

- die Unterstützung von Standard-APIs für Applikationsentwickler,
- die Unterstützung von Applikationsentwicklungen durch Services für CTI, Management und Lizenzierung, verfügbar über ein SDK,
- die Unterstützung der Migration von HiPath 4000 mit vielfacher Verbindung zu unterschiedlichen Kommunikationsplattformen, die eine Applikation nahezu unabhängig von der darunterliegenden Infrastruktur macht.

Die folgende Grafik zeigt die Grundstruktur der HiPath CAP mit detaillierten Informationen über die unterstützten Protokolle und Kodierungsvarianten, die CAP internen Services und einige unterstützte TK-Anlagen.



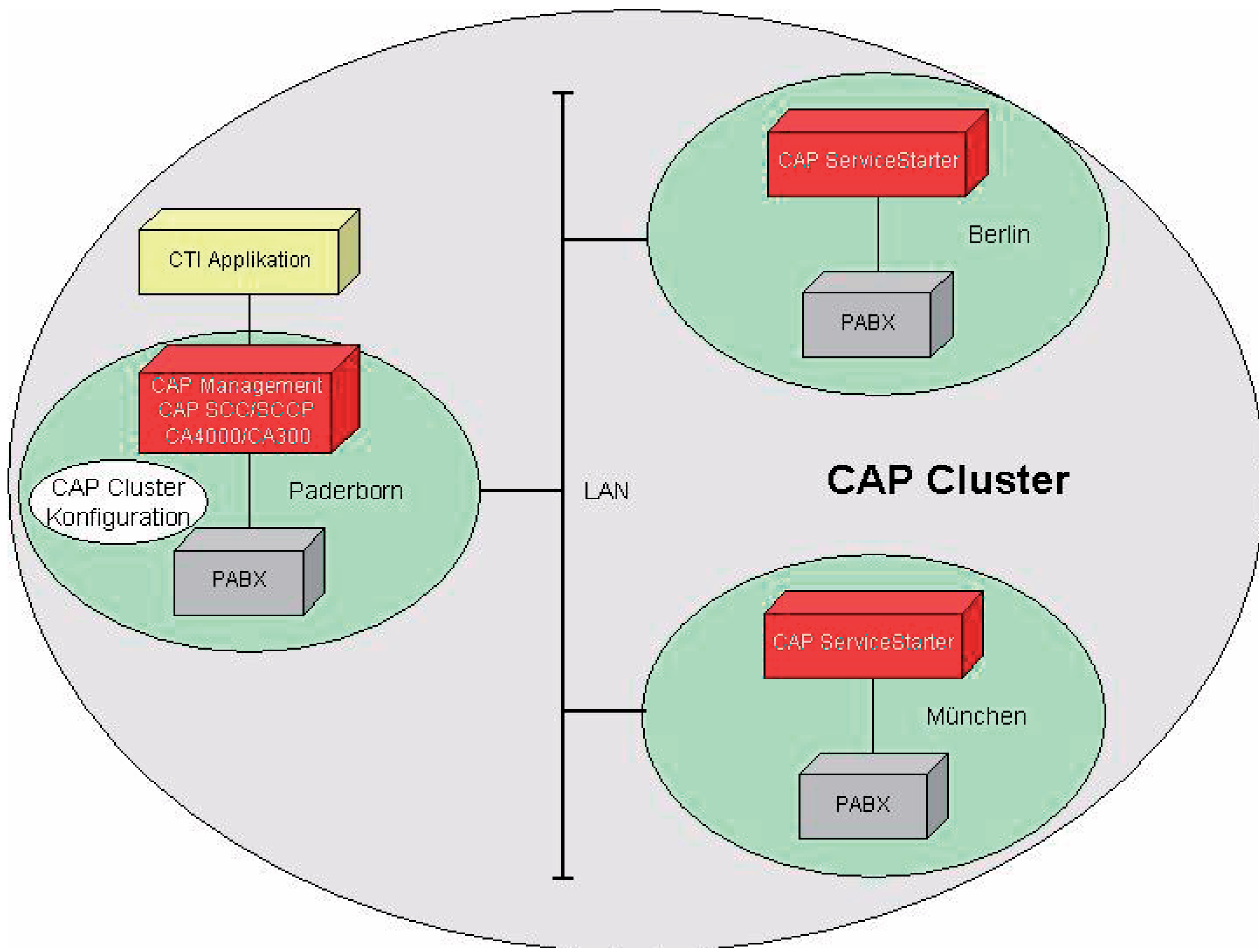
Highlights

- Standard Protokolle und API´s: Microsoft TAPI 2.x/3.0, JTAPI, CSTA III ASN.1, CSTA XML, Microsoft Wave API
- Call Control Service (SCC) für CTI
  - Multi Domain Leistungsmerkmale
  - Harmonisierung der Call-Modelle der Hicom 300 H, HiPath 3000, HiPath 4000, HiPath 5000, HiPath 8000, Octopus E300/800 Rel. 6.5/10, Realitis, Alcatel, Nortel Meridian, Cisco und Avaya - für TAPI und CSTA basierende Applikationen
- Media Service (MEB) für CTI
  - Media Streaming als neues HiPath CAP-Leistungsmerkmal für Applikationen
- Fault Management Service
  - Integration in das HiPath Management (vom CAP Management unabhängig)
- Lizenz-, Benutzer-, und Konfigurations-Management Services
  - Einheitliche Lizenzstruktur
  - Integriertes Lizenz- und Benutzermanagement
  - Anbindung an den HiPath Lizenzserver (CLS)
  - LM als ein Service um HiPath CAP und Applikationen in gleicher Weise zu lizenzieren
- Unterstützung spezieller Leistungsmerkmale
  - LiRus, AP emergency, XML PhoneServices

5.3 HiPath CAP Management

Das CAP Management ist die zentrale Komponente in einem CAP Cluster. Es administriert und steuert alle Prozesse und Services in einer lokalen oder einer verteilten HiPath CAP Installation. Die Cluster ID ist eine eindeutige Kennzeichnung von CAP Komponenten in dem gleichen CAP Cluster.

Das nachfolgende Schaubild verdeutlicht die Lage und Konfiguration der einzelnen CAP Komponenten bei einer verteilten Installation.



Das CAP Management wird durch den Windows Dienst **HiPath CTI** gestartet und bietet zur Administration eine Web-basierte Oberfläche.

Aufgaben des CAP Managements

- Administration von zentralen und verteilten Komponenten
- Administration von Benutzern
- Administration von Devices
- Administration von Lizenzen
- Lizenzüberprüfung und Zugriffkontrollen von Benutzern und Devices
- Verwaltung von Statusinformationen der verschiedenen Prozesse und Services

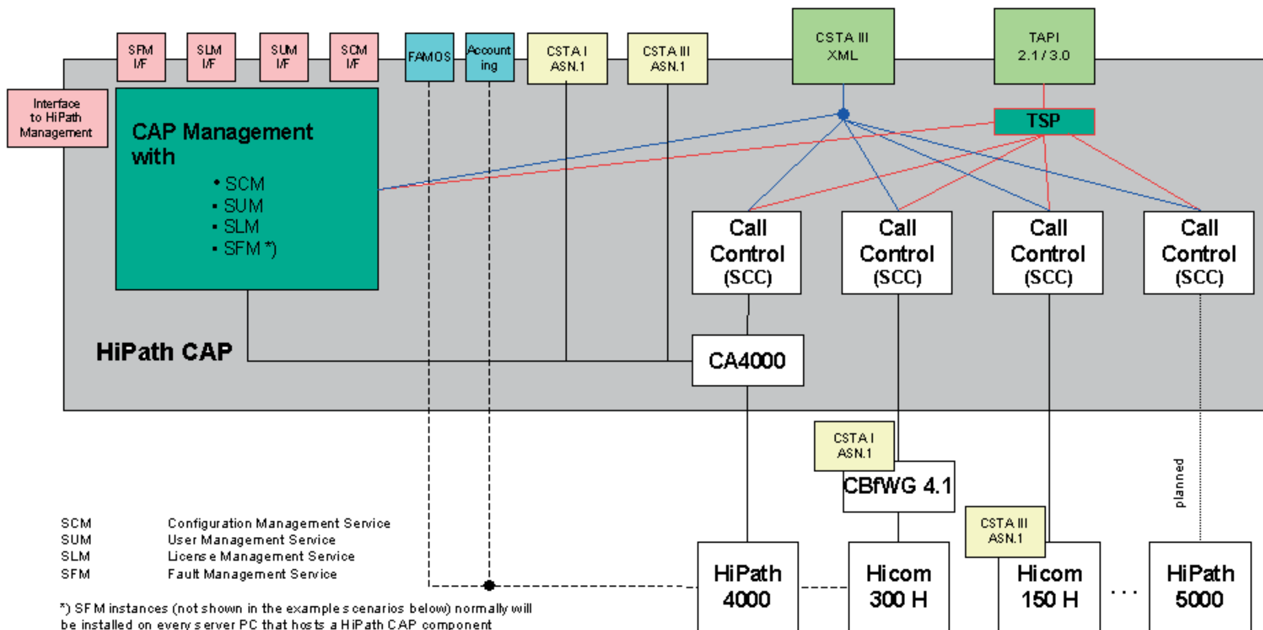
Services des HiPath CAP Managements

Das CAP Management kann in verschiedene Services aufgeteilt werden, welche unterschiedliche Aufgaben haben:

- Konfigurationsmanagement (SCM)
- Benutzermanagement (SUM)
- Lizenzmanagement (SLM)
- CallIdRepository
- Address Translation Service (SAT)
- Open LDAP Server
- FaultManagement (SFM) (vom CAP Management unabhängig)

5.3.1 HiPath CAP-Client/Server Architektur

Dem HiPath CAP-System liegt eine Client/Server Architektur zu Grunde. Diese Architektur ermöglicht die Realisierung von 3rd Party CTI-Lösungen. CAP Call Control Service realisiert die Verbindung zur TK-Anlage und stellt Anwendungsschnittstellen sowohl auf dem CTI-Server als auch an den CTI-Arbeitsplätzen zur Verfügung.



Die Gesamtarchitektur umfasst drei Komponenten:

- TK-Anlage
- CTI-Server auf Basis CSTA
- CTI-Client auf Basis Microsoft TAPI

Die von dem HiPath CAP-System unterstützten TK-Anlagen unterscheiden sich insbesondere im Umfang der über CSTA verfügbaren Telefoniefunktionalität und der Art der physikalischen Verbindung zwischen TK-Anlage und CTI-Server.

Das HiPath CAP-System für sich besteht aus der Server-Komponente CAP Management, CAP Call Control Service und der Client-Komponente CAP TAPI Service Provider. Für jede der Komponenten gibt es jeweils eine eigene Installationsroutine.

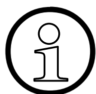
Mehrere TK-Anlagen können in einem Verbund von CAP Call Control Services (pro TK-Anlage ein Service) gesteuert werden.

CAP Call Control Service läuft in Verbindung mit CAP Management, das die Administration der einzelnen Server ermöglicht. Ausserdem werden über CAP Management alle Telefonnummern mit einem Passwort geschützt.

CAP Call Control Service läuft in Verbindung mit CAP Management, das die Administration der einzelnen Server ermöglicht. Ausserdem werden über CAP Management alle Telefonnummern mit einem Passwort geschützt.

Die Verbindungsaufnahme zwischen HiPath 2000 V1.0 und CAP Call Control Service erfolgt indirekt über CAP Management. In CAP Management erfolgt die Authentifizierung über Passwort und die Ermittlung des für eine Leitung zuständigen CAP Call Control Servers. Damit sind Umkonfigurationen auf Seiten der TK-Anlagen transparent für die HiPath 2000 V1.0 und die Client-Anwendungen auf Basis dieses Service Providers.

Wenn etwa Telefonnummern von einer TK-Anlage auf eine andere verlagert und damit auch ein anderer CAP Call Control Server (mit anderer IP-Adresse/Portnummer) zuständig wird, ist nur die entsprechende Konfiguration über CAP Management durchzuführen.
Umgekehrt ist keinerlei Konfiguration von Client Anwendungen im HiPath CAP-System erforderlich. So können sich IP-Adressen von Clients beliebig ändern, etwa durch dynamische Zuteilung über DHCP. Bei jedem Anmelden erfolgt erneut die dynamische Zuordnung von Client und CAP Call Control Service über CAP Management.



Weiterführende Informationen zum Thema CAP entnehmen Sie bitte den folgenden Manualen:

- HiPath CAP 3.0, Installations- und Administrationshandbuch
- HiPath CAP 3.0, CAP TAPI Service Provider, Installations- und Administrationshandbuch

5.4 CAP TAPI Service Provider

Das HiPath CAP ist eine Softwareplattform für Computer Telephony Integration (CTI) an TK-Anlagen. Über die HiPath 2000 V1.0 können CTI-Clientanwendungen angebunden werden.

Das HiPath CAP-System stellt die Funktionalität der TK-Anlage über Schnittstellen zur Verfügung, die damit in beliebigen CTI-Anwendungen genutzt werden kann.

6 Workpoint Clients

Folgende Themen finden Sie in diesem Kapitel:

6.1 DSL-Telefonie (Voice over IP)

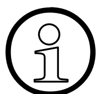
6.1.1 Einführung

Voice over IP (VoIP) ermöglicht die Übertragung von Sprachdaten über IP-gestützte Netze (paketorientierte Netze).

Um Anrufe zu tätigen, ist eine Kommunikation zwischen den beteiligten Workpoints bereits im Vorfeld eines Gesprächs notwendig. Diese als Signalisierung bezeichnete Kommunikation ist möglich über

- den übergreifenden Standard H.323.
  Neben Protokollen für die Signalisierung gehören zu diesem Standard Protokolle für den Austausch von Workpoint-Funktionalitäten, für die Verbindungskontrolle, für den Austausch von Statusinformationen und für die Datenflusskontrolle.
  H.323 haftet der Nachteil eines komplexen, starr definierten Multimedia-Systemkonzepts an, das für flexible Einsätze außerhalb üblicher Telefonie- und Videokonferenzanwendungen wenig geeignet ist.
- das SIP (Session Initiation Protocol)-Protokoll.
  Das SIP-Protokoll ist ein ASCII-basierendes Signalprotokoll, dass zur Einrichtung von Sitzungen in einem IP-Netz verwendet wird.
  Das SIP-Protokoll lehnt sich an bekannte Internet-Technologien wie HTML und E-Mail an und schafft eine nahtlose Integration in die Internet-Protokollarchitektur. SIP behält sich dabei unterschiedlichste Einsatzszenarien vor und beschränkt sich auf Signalisierungsaufgaben. Deshalb kann SIP, gemeinsam mit anderen Protokollen, für verschiedene Zwecke eingesetzt werden.

Am VoIP-Markt hat sich inzwischen das SIP-Protokoll gegenüber H.323 durchgesetzt. Die wichtigsten Internet Telephony Service Provider (ITSP) setzen fast alle ausschließlich SIP ein.



Der in dieser Dokumentation verwendete Begriff DSL-Telefonie bezieht sich auf das Telefonieren über IP-gestützte Netze (Voice over IP) und eine Signalisierung mittels SIP-Protokoll.

Gateway, Gatekeeper, Registrar, SIP-Server

In HiPath 2000 sind folgende Funktionen integriert:

- Gateway
- Gatekeeper
- Registrar
- SIP-Server (BacktoBack User Agent)

Gateways werden benötigt, um die Kommunikation zwischen IP-gestützten Netzen (LAN, Intranet, Internet) und leitungsvermittelten Netzen (ISDN, PSTN) zu ermöglichen.

Ein Gatekeeper hat unter anderem folgende Aufgaben:

- Registrierung der IP-Workpoints (H323):
  - System Clients, wie optiClient 130, optiPoint 410, optiPoint 420, optiPoint 600
  - H.323 Clients, wie zum Beispiel AP1120
  - Aufbau einer Verbindung
  - Zugangskontrolle

Ein Registrar wird benötigt, um SIP-Clients, wie optiPoint 150 S, optiPoint 410 S, optiPoint 420 S am System anzumelden.

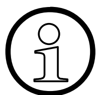
Ein SIP-Server übernimmt die Aufgabe des Verbindungssteuerung und der Zugangskontrolle.

6.1.2 DHCP (Dynamic Host Configuration Protocol)-Server

Das DHCP-Protokoll ist ein Client-Server-Protokoll, das den Aufwand für die Vergabe von IP-Adressen und sonstigen Parametern reduziert. Über den in HiPath 2000 implementierten DHCP-Server kann ein Administrator alle TCP/IP-Konfigurations-Parameter zentral verwalten und warten. Das DHCP-Protokoll dient der dynamischen und automatischen Workpoint-Konfiguration, zum Beispiel der Vergabe von IP-Adressen.

Die Administration des DHCP-Servers erfolgt über das WBM. Folgende Funktionalitäten werden unterstützt:

- Konfiguration des DHCP-Servers (Aktivieren/Deaktivieren)
- Konfiguration der DHCP-Client Start-IP-Adressbereiche
- Reservierung von IP-Adressen für bestimmte MAC-Adressen
- Lease Time Konfiguration
- Anzeige reservierter DHCP-Client-Adressen im WBM
- DNS Address Settings und Übertragung
- Default Gateway Settings und Übertragung



Der HiPath 2000-interne DHCP-Server unterstützt ausschließlich die LAN-Schnittstellen. Workpoints, die über die WAN- oder DMZ-Schnittstelle angeschlossen sind, können nicht auf den DHCP-Server zugreifen.

6.1.3 BOOTP (Bootstrap Protocol)-Server

Das Bootstrap-Protokoll ist ein Client-Server-Protokoll, das der Vergabe von IP-Adressen dient. Es kann überall dort eingesetzt werden, wo die Adressvergabe über das Netz erfolgen muss.

Beim BOOTP-Protokoll benutzen BootP-Client und -Server das UDP-Protokoll zur Kommunikation. Dabei geht es im Wesentlichen um den Austausch eines Datenpaketes, in dem der BOOTP-Server dem Client wesentliche Informationen übermittelt.

Die BOOTP-Server-Funktionalität wird durch HiPath 2000 parallel zum DHCP-Server angeboten und unterstützt nur die Versorgung von älteren, nicht DHCP-fähigen Endeinrichtungen (zum Beispiel Drucker) mit einer gültigen IP-Adresse.

Der BOOTP-Server hat keine eigene Oberfläche und kann nicht administriert werden.

6.1.4 DSL-Telefonie mit HiPath 2000 nutzen

Der Anschluss der HiPath 2000 an einen Internet Telephony Service Provider (ITSP) und damit die Nutzung der DSL-Telefonie kann über einen DSL-Telefonie-Teilnehmeranschluss (ab V1.0 SMR-06) oder einen DSL-Telefonie-Anlagenanschluss mit Durchwahl (ab V1.0 SMR-09) erfolgen.

- **DSL-Telefonie-Teilnehmeranschluss**

  Hierbei handelt es sich um einen Anschluss, bei dem jede Rufnummer einzeln beim ITSP registriert werden muss. HiPath 2000 unterstützt die Anbindung an einen ITSP für Standalone-Systeme. Die Konfiguration verschiedener ITSPs ist möglich, jedoch kann maximal ein ITSP aktiv sein. Ein Umschalten auf einen anderen ITSP ist möglich. Bis zu 30 ITSP-Benutzerkennungen (ITSP Client User Accounts) können eingerichtet werden. Die ITSP-Benutzerkennungen und die DSL-Telefonie-Teilnehmerrufnummern werden nach Beantragung des DSL-Telefonie-Zugangs durch den Provider bereitgestellt.

  Parallel werden sowohl S_0-Verbindungen als auch ITSP-Verbindungen über das Internet unterstützt. Per Default werden alle Verbindungen (außer Notrufe und Sonderrufnummern, Fax- und Modemverbindungen) über den ITSP geführt. Im Überlauf werden ISDN-Verbindungen genutzt.

  Für die Verbindung zum Internet muss HiPath 2000 als Router fungieren.

  Bei allen Vernetzungslösungen (HiPath 2000 untereinander oder HiPath 2000 mit HiPath 3000, HiPath 4000, HiPath 5000) werden ausschließlich S_0-Amtsanschlüsse verwendet. Die gleichzeitige Nutzung von Vernetzungen über CorNet-IP und ITSP-Anschlüsse wird nicht unterstützt.

NEU ab V1.0 SMR-09:
Die parallele Anbindung und Nutzung von bis zu vier ITSPs ist möglich. Über die Leitweglenkung kann anhand der gewählten Rufnummer und der aktuellen Uhrzeit eine Priorisierung der eingerichteten ITSPs erfolgen.

Die Verbindung zum Internet kann direkt (HiPath 2000 fungiert als Router) oder über einen vorhandenen Kunden-Router und/oder eine vorhandene Firewall erfolgen.

Bei einer Vernetzung von HiPath 2000-Systemen untereinander oder HiPath 2000- mit HiPath 3000-Systemen wird eine zentrale ITSP-Anbindung unterstützt. Hierbei ist die parallele Anbindung und Nutzung von bis zu vier ITSPs möglich.

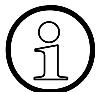
- **DSL-Telefonie-Anlagenanschluss mit Durchwahl** (ab V1.0 SMR-09)

  Hierbei handelt es sich um einen durchwahlfähigen Anschluss, für den ein ITSP eine DSL-Telefonie-Anlagenrufnummer, eine ITSP-Benutzerkennung für die Anlage und ein Rufnummernband mit DSL-Telefonie-Teilnehmerrufnummern bereitstellt. Bis zu 30 DSL-Telefonie-Teilnehmerrufnummern können im System eingerichtet werden.

  Die parallele Anbindung und Nutzung von bis zu vier ITSPs ist möglich. Über die Leitweglenkung kann anhand der gewählten Rufnummer und der aktuellen Uhrzeit eine Priorisierung der eingerichteten ITSPs erfolgen.

  Die Verbindung zum Internet kann direkt (HiPath 2000 fungiert als Router) oder über einen vorhandenen Kunden-Router und/oder eine vorhandene Firewall erfolgen.

  Bei einer Vernetzung von HiPath 2000-Systemen untereinander oder HiPath 2000- mit HiPath 3000-Systemen wird eine zentrale ITSP-Anbindung unterstützt. Hierbei ist die parallele Anbindung und Nutzung von bis zu vier ITSPs möglich.



Bei Ausfall eines ITSPs oder des Internets kann mittels Least Cost Routing LCR die Verbindung über ISDN-Anschlüsse sichergestellt werden.
Sonderrufnummen und Notrufnummern, die Provider-abhängig nicht unterstützt werden, sind über S_0-Anschlüsse zu führen.

Verbindung zum Internet (zum ITSP)

Bei beiden genannten Anschlussarten kann die HiPath 2000 sowohl direkt als auch über einen vorhandenen Kunden-Router und/oder eine vorhandene Firewall mit derm Internet verbunden werden.

- HiPath 2000 mit direktem Internetzugang

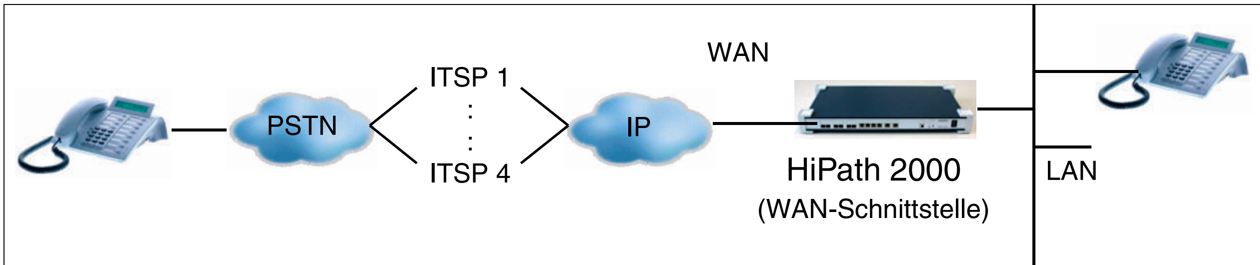


Bild 6-1 HiPath 2000 mit direktem Internetzugang

- HiPath 2000 als Client im Kundennetz: Internetzugang über vorhandene Infrastruktur (Router / Firewall) des Kunden

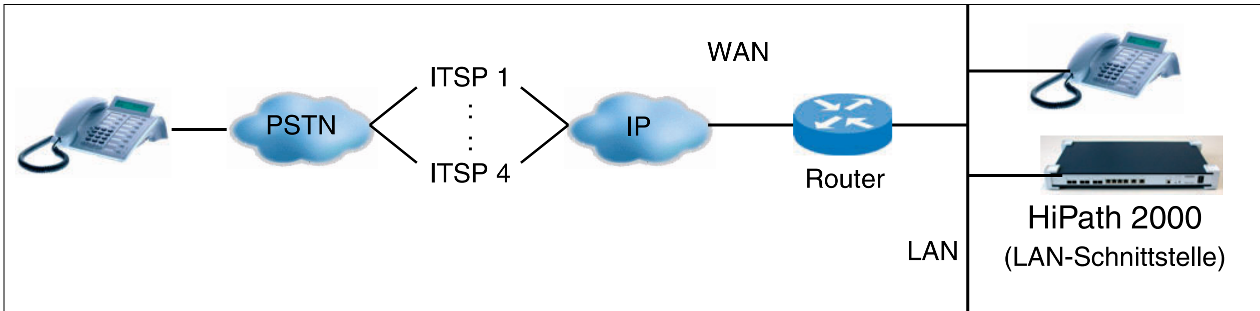


Bild 6-2 HiPath 2000 als Client im Kundennetz: Internetzugang über vorhandene Infrastruktur (Router / Firewall) des Kunden

Bei Integration einer HiPath 2000 in eine vorhandene Infrastruktur (Router / Firewall) des Kunden ist folgendes zu beachten:

Die Ankopplung des Kunden-LAN an das Internet erfolgt über einen vorhandenen Router und/oder eine vorhandene Firewall. HiPath 2000 wird als Komponente in das interne LAN des Kunden integriert.

Um eine gute Sprachqualität zu gewährleisten, muss der beim Kunden eingesetzte Router über QoS-Funktionen und Mechanismen zur Bandbreitenkontrolle verfügen.

Typischerweise wird in diesem Umfeld **NAT (Network Address Translation)** eingesetzt. Dabei handelt es sich um ein Verfahren, um eine IP-Adresse in einem Datenpaket durch eine andere zu ersetzen. Häufig wird dies benutzt, um private IP-Adressen auf öffentliche IP-Adressen abzubilden. In diesem Fall bedeutet das, die im Kunden-LAN verwendeten IP-Adressen nicht im Internet sichtbar sind, sondern vom Router oder von der Firewall über deren NAT-Funktion ersetzt werden.

Um Datenpakete empfangen zu können (um kommende Gespräche über das Internet empfangen zu können), muss der betreffende IP-Workpoint seine im Internet verwendete öffentliche IP-Adresse ermitteln und mitteilen können. Dies ist nötig, damit der rufende Teilnehmer seine Gesprächsdaten korrekt adressieren kann. Das ist über einen vom ITSP betriebenen STUN-Server möglich. **STUN (Simple Traversal of UDP over NATs = einfaches Überqueren von UDP über NAT)** ist ein Netzwerkprotokoll, um das Vorhandensein und die Art von NAT-Firewalls und NAT-Routern zu erkennen.

Durch eine Verbindung mit dem STUN-Server kann ein IP-Workpoint seine derzeit gültige öffentliche IP-Adresse ermitteln und mitteilen. Der IP-Workpoint ist dann aus dem Internet erreichbar, ohne die Einstellungen der NAT-Firewall oder des NAT-Routers zu verändern.

Die Konfiguration des Systems für die Anbindung an einen ITSP erfolgt über das Web-based Management WBM. Für die bereits freigegebenen Provider wird eine vereinfachte Administration anhand von Einrichtassistenten angeboten.

Eine detaillierte Beschreibung der Vorgehensweise bei der Administration enthält die HiPath 2000 V1.0 Installationsanleitung.

6.2 optiClient 130 V5.0

Der optiClient 130 V5.0 ist eine auf dem PC ablauffähige Multimedia-Applikation, die Verbindungsdienste verschiedener Kommunikationsmedien über LAN (Netzwerk) anbietet. Sprach-, Video- oder Chat-Verbindungen können mit dem optiClient 130 V5.0 verwaltet und gesteuert werden. Für Sprachverbindungen bedeutet dies, dass der optiClient 130 V5.0 über einen PC wie ein Telefon genutzt werden kann.

Modularer Aufbau

Der optiClient 130 V5.0 verfügt über einen modularen Aufbau von Funktionselementen, die grundsätzlich für eine Erweiterung des Funktionsumfangs ergänzt oder auch ausgetauscht werden können.

- Das Basismodul des optiClient 130 V5.0 ist die sogenannte Hauptleiste. Die Hauptleiste selbst bietet keine Kommunikationsfunktionen, sondern dient als zentrales Element, das mit den verschiedenen Modulen zusammen die Kommunikationsfunktionen und die Darstellung des optiClient 130 V5.0 bestimmt.
- Oberflächen-Module sind die Module, mit denen die verfügbaren Funktionen in Fenstern und Dialogen bedient werden können. Oberflächen-Module sind zum Beispiel: Telefon-Fenster, Verzeichnisse, Ruflistenverwaltung, etc.
- Provider-Module bestimmen, an welche Kommunikationssysteme oder Kommunikations-dienste- Anbieter (Provider) der optiClient 130 V5.0 angebunden werden kann.
- Manager-Module wirken nicht sichtbar im Hintergrund. Sie übernehmen allgemeine Steuerungsfunktionen rund um die Kommunikation. Manager-Module sind zum Beispiel der Keyboard-Manager und der ScreenSaver-Manager.

PC-Voraussetzungen

- Betriebssystem Windows 2000 (ab SP 4) oder Windows XP (SP 1)
- Prozessor: empfohlen ab 1 GHz
- RAM-Speicher: mindestens 512 MB

Dokumentation

Die Dokumentation ist in 7 Sprachen verfügbar.

6.3 optiPoint 410 / optipoint 410 S und optiPoint 420 / optiPoint 420 S

Einführung

Die IP-Telefone der optiPoint 410/optiPoint 410 S- und der optiPoint 420/optiPoint 420 S-Familien ermöglichen dem Anwender, Telefongespräche auf einfache und gewohnte Art über ein Datennetz zu führen.

Eine komfortable und interaktive Bedienung wird durch drei Dialogtasten in Verbindung mit der Displayanzeige gewährleistet (nicht optiPoint 410 entry und optiPoint 410 entry S). Darüber hinaus visualisiert das Tasten-Lampen-Prinzip die aktivierten Funktionen.

Der Unterschied zwischen den optiPoint 410/optiPoint 410 S- und den optiPoint 420/optiPoint 420 S-Familien liegt in der Ausführung der Funktionstastenfelder:

- optiPoint 410/optiPoint 410 S-Familien: Die Funktionstasten verfügen über Tastenfelder mit Beschriftungsstreifen, auf die die aktuell gespeicherte Funktion oder Rufnummer eingetragen werden kann.
- optiPoint 420/optiPoint 420 S-Familien: Bei den Funktionstasten handelt es sich um Self-Labeling Keys. Self-Labeling bedeutet, dass jeder Taste ein Display (1 Zeile mit 12 Zeichen) zugeordnet ist, in dem die aktuell gespeicherte Funktion oder Rufnummer angezeigt wird.

Durch das Beistellgerät optiPoint self labeling key module kann die Anzahl der zur Verfügung stehenden Funktionstasten bei den Endgerätetypen standard und advance erhöht werden. Auch die Beistellgeräte optiPoint key module und optiPoint BLF können zusammen mit den Familien optiPoint 410/optiPoint 410 S- und optiPoint 420/optiPoint 420 S genutzt werden.

Durch den Einsatz verschiedener optiPoint 500-Adapter wird eine flexible Erweiterung des Telefonarbeitsplatzes ermöglicht (nicht bei den Endgerätetypen entry, economy und economy plus).

Unterschiede zwischen den optiPoint 410/optiPoint 420- und den optiPoint 410 S/optiPoint 420 S-Familien:

- optiPoint 410/optiPoint 420-Familien: Alle Leistungsmerkmale der HiPath 2000 können genutzt werden (außer Relocate/Rufnummerntausch), die im Dialog mit dem Display, im Service-Menü und auf Funktionstasten angeboten werden.
- optiPoint 410 S/optiPoint 420 S-Familien: Die zugehörigen Endgeräte unterstützen das SIP (Session Initiation Protocol)-Protokoll. Das SIP-Protokoll ist ein ASCII-basierendes Signalprotokoll, dass zur Einrichtung von Sitzungen in einem IP-Netz verwendet wird. Hinweis: Der in dieser Dokumentation verwendete Begriff DSL-Telefonie bezieht sich auf das Telefonieren über IP-gestützte Netze (Voice over IP) und eine Signalisierung mittels SIP-Protokoll.

  Folgende Leistungsmerkmale für DSL-Telefonie-Teilnehmer werden aktiv unterstützt:

- CLIP (Anzeige der Rufnummer des rufenden Teilnehmers beim gerufenen Teilnehmer)
- CLIR (Unterdrückung der Rufnummernanzeige des rufenden Teilnehmers beim gerufenen Teilnehmer)
- COLP (Anzeige der Rufnummer des gerufenen Teilnehmers beim rufenden Teilnehmer)
- COLR (Unterdrückung der Rufnummernanzeige des gerufenen Teilnehmers beim rufenden Teilnehmer)
- Rückfrage
- Halten
- Makeln
- Übergeben (Übergeben nach Melden)
- DISA (Direct Inward System Access): Es können keine Leistungsmerkmale für das SIP-Endgerät aktiviert werden.
- Inband DTMF

Folgende Leistungsmerkmale können DSL-Telefonie-Teilnehmer zwar nicht aktivieren, sie können allerdings passiv eingebunden werden:

- Anrufumleitung (Umleitung auf einen DSL-Telefonie-Teilnehmer wird unterstützt.)
- Konferenz (DSL-Telefonie-Teilnehmer kann passiv eingebunden werden.)
- Parken (DSL-Telefonie-Teilnehmer können geparkt werden. Aus Sicht des DSL-Telefonie-Teilnehmers ist dies wie “Halten”.)
- Live Call Recording (DSL-Telefonie-Teilnehmer kann passiv eingebunden werden.)
- Diskretes Ansprechen (DSL-Telefonie-Teilnehmer kann passiv eingebunden werden.)
- Automatische Berechtigungsumschaltung (DSL-Telefonie-Teilnehmer kann in automatische Berechtigungsumschaltung eingebunden werden.)
- Verkehrsbeziehungsgruppen (DSL-Telefonie-Teilnehmer kann in VBZ-Gruppen einbezogen werden.)

Folgende Einschränkungen für DSL-Telefonie-Teilnehmer sind zu beachten:

- DSL-Telefonie-Teilnehmer sind bei HiPath 2000 V1.0 als DSS1 (funktionales Endgerät) konfiguriert und können daher nicht vom System überwacht werden (kein Monitoring). DSL-Telefonie-Teilnehmer können keine Applikationen nutzen, für die ein Monitoring erforderlich ist (zum Beispiel HiPath ComAssistant).

- Die Einbindung von DSL-Telefonie-Teilnehmern in Anrufübernahmegruppen, Sammelanschlüsse, Team-, Top- oder MULAP-Gruppen ist nicht möglich.
- DSL-Telefonie-Teilnehmer können keine Systemleistungsmerkmale aktivieren oder nutzen, die über Kennzahlen gesteuert werden können.
- Wird ein DSL-Telefonie-Teilnehmer gehalten, wird MOH eingespielt. Bei Übergabe vor Melden des DSL-Telefonie-Teilnehmers an einen anderen Teilnehmer, wird dem DSL-Telefonie-Teilnehmer kein MOH oder Rufton eingespielt.
- Wird ein geparkter DSL-Telefonie-Teilnehmer nicht von dem Teilnehmer entparkt, der ihn geparkt hat, wird das Display des DSL-Telefonie-Teilnehmers nicht aktualisiert.
- SIP-Endgeräte werden nicht vom HiPath 2000-internen Deployment Service unterstützt.
- Unter Umständen können endgerätespezifische Leistungsmerkmale an HiPath 2000 V1.0 nicht genutzt werden. Dies schließt Leistungsmerkmale ein, die über die Menüoberfläche des Endgerätes angeboten werden. Generell freigeben sind die Leistungsmerkmale, die über das Grundsystem HiPath 2000 V1.0 angeboten werden.

6.3.1 optiPoint 410/410 S

6.3.1.1 optiPoint 410 entry, optiPoint 410 entry S

Wesentliche Merkmale

- Protokolle
  - H.323, HFA/V3 + V4, CorNet-IP, SIP
  - HTTP, DHCP, SNMP, FTP
  - H.235 (Security)
  - QoS nach DIFFSERV und IEEE 802.1 p/Q
- Sprachkomprimierung G.711, G.722, G.723 und G.729 A/B
- Power over LAN (gemäß Cisco und Standard pre802.3af)
- CTI (zum Beispiel über TAPI 3rd Party)
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den LAN-Anschluss
- 8 Funktionstasten mit Leuchtdioden
- 2 Einstelltasten (Plus/Minus) für Lautstärke und Klangfarbe
- zur Wandmontage geeignet
- keine Modularität (keine Anschlussmöglichkeit für Adapter oder Bestellgeräte), kein Display



Bild 6-3 optiPoint 410 entry, optiPoint 410 entry S

6.3.1.2 optiPoint 410 economy, optiPoint 410 economy S

Wesentliche Merkmale

- Protokolle
  - H.323, HFA/V3 + V4, CorNet-IP, SIP
  - HTTP, DHCP, SNMP, FTP
  - H.235 (Security)
  - QoS nach DIFFSERV und IEEE 802.1 p/Q
- Sprachkomprimierung G.711, G.722, G.723 und G.729 A/B
- Power over LAN (gemäß Cisco und Standard pre802.3af)
- CTI (zum Beispiel über TAPI 3rd Party)
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den LAN-Anschluss
- 12 Funktionstasten mit Leuchtdioden
- Alphanumerisches LCD-Display (schwenkbar) mit 2 Zeilen zu je 24 Zeichen
- 3 Dialogtasten zur interaktiven Benutzerführung: “Ja”, “Zurück” und “Weiter”
- Lauthören
- 2 Einstelltasten (Plus/Minus) für Lautstärke, Klangfarbe und Displaykontrast
- zur Wandmontage geeignet
- keine Modularität (keine Anschlussmöglichkeit für Adapter oder Bestellgeräte)

6.3.1.3 optiPoint 410 economy plus, optiPoint 410 economy plus S

hat zwei zusätzliche Leistungsmerkmale gegenüber dem optiPoint 410 economy. Dieses Telefon ist ideal für den Einsatz im Büro oder Call-Center.

- 10/100 Mbit/s Mini-Switch
- 1 Hör-Sprechgarnituranschluss (121TR9-5/Polaris)



Bild 6-4 optiPoint 410 economy, optiPoint 410 economy S

6.3.1.4 optiPoint 410 standard, optiPoint 410 standard S

Wesentliche Merkmale

- Protokolle
  - H.323, HFA/V3 + V4, CorNet-IP, SIP
  - HTTP, DHCP, SNMP, FTP
  - H.235 (Security)
  - QoS nach DIFFSERV und IEEE 802.1 p/Q
- Sprachkomprimierung G.711, G.722, G.723 und G.729 A/B
- Power over LAN (gemäß Cisco und Standard pre802.3af)
- CTI (zum Beispiel über TAPI 1st Party)
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den LAN-Anschluss
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den PC-Anschluss
- 12 Funktionstasten mit Leuchtdioden
- Alphanumerisches LCD-Display (schwenkbar) mit 2 Zeilen zu je 24 Zeichen
- 3 Dialogtasten zur interaktiven Benutzerführung: “Ja”, “Zurück” und “Weiter”
- Vollduplex-Freisprechen mit Echo-Unterdrückung zur Raumadaption
- Anschluss für Hör-/Sprechgarnitur (121 TR 9-5)
- 2 Einstelltasten (Plus/Minus) für Lautstärke, Klangfarbe, Freisprechqualität und Display-kontrast
- Modularität:
  - 2 Adaptersteckplätze
  - 1 Schnittstelle für max. 2 Beistellgeräte
- zur Wandmontage geeignet



Bild 6-5 optiPoint 410 standard, optiPoint 410 standard S

6.3.1.5 optiPoint 410 advance, optiPoint 410 advance S

Wesentliche Merkmale

- Protokolle
  - H.323, HFA/V3 + V4, CorNet-IP, SIP
  - HTTP, DHCP, SNMP, FTP
  - H.235 (Security)
  - QoS nach DIFFSERV und IEEE 802.1 p/Q
- Sprachkomprimierung G.711, G.722, G.723 und G.729 A/B
- Power over LAN (gemäß Cisco und Standard pre802.3af)
- CTI (zum Beispiel über TAPI 1st Party)
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den LAN-Anschluss
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den PC-Anschluss
- 1 integrierte USB-1.1-Schnittstelle
- 19 Funktionstasten mit Leuchtdioden
- Grafik-Display (schwenkbar) mit 4 Zeilen zu je 24 Zeichen
- 3 Dialogtasten zur interaktiven Benutzerführung: “Ja”, “Zurück” und “Weiter”
- Vollduplex-Freisprechen mit Echo-Unterdrückung zur Raumadaption
- Anschluss für Hör-/Sprechgarnitur (121 TR 9-5)
- 2 Einstelltasten (Plus/Minus) für Lautstärke, Klangfarbe, Freisprechqualität und Display-kontrast
- Modularität:
  - 1 Adaptersteckplatz
  - 1 Schnittstelle für max. 2 Beistellgeräte
- zur Wandmontage geeignet



Bild 6-6 optiPoint 410 advance, optiPoint 410 advance S

6.3.2 optiPoint 420/420 S

Die IP-Telefone der optiPoint 420-Familie verfügen über Self-Labeling Keys. Self-Labeling bedeutet, dass jeder Taste ein Display (1 Zeile mit 12 Zeichen) zugeordnet ist, in dem die aktuell gespeicherte Funktion oder Rufnummer angezeigt wird.

6.3.2.1 optiPoint 420 economy, optiPoint 420 economy S

Wesentliche Merkmale

- Protokolle
  - H.323, HFA/V3 + V4, CorNet-IP, SIP
  - HTTP, DHCP, SNMP, FTP
  - H.235 (Security)
  - QoS nach DIFFSERV und IEEE 802.1 p/Q
- Sprachkomprimierung G.711, G.722, G.723 und G.729 A/B
- Power over LAN (gemäß Cisco und Standard pre802.3af)
- CTI (zum Beispiel über TAPI 1st Party)
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den LAN-Anschluss
- 12 Funktionstasten mit Leuchtdioden und Self-Labeling Keys
- Grafik-Display (schwenkbar) mit 2 Zeilen zu je 24 Zeichen
- 3 Dialogtasten zur interaktiven Benutzerführung: “Ja”, “Zurück” und “Weiter”
- Lauthören
- 2 Einstelltasten (Plus/Minus) für Lautstärke, Klangfarbe und Displaykontrast
- zur Wandmontage geeignet
- keine Modularität (keine Anschlussmöglichkeit für Adapter oder Bestellgeräte)



Bild 6-7 optiPoint 420 economy, optiPoint 420 economy S

6.3.2.2 optiPoint 420 economy plus, optiPoint 420 economy plus S

Wesentliche Merkmale

- Protokolle
  - H.323, HFA/V3 + V4, CorNet-IP, SIP
  - HTTP, DHCP, SNMP, FTP
  - H.235 (Security)
  - QoS nach DIFFSERV und IEEE 802.1 p/Q
- Sprachkomprimierung G.711, G.722, G.723 und G.729 A/B
- Power over LAN (gemäß Cisco und Standard pre802.3af)
- CTI (zum Beispiel über TAPI 1st Party)
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den LAN-Anschluss
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den PC-Anschluss
- 12 Funktionstasten mit Leuchtdioden und Self-Labeling Keys
- Grafik-Display (schwenkbar) mit 2 Zeilen zu je 24 Zeichen
- 3 Dialogtasten zur interaktiven Benutzerführung: “Ja”, “Zurück” und “Weiter”
- Lauthören
- Anschluss für Hör-/Sprechgarnitur (121 TR 9-5)
- 2 Einstelltasten (Plus/Minus) für Lautstärke, Klangfarbe und Displaykontrast
- zur Wandmontage geeignet
- keine Modularität (keine Anschlussmöglichkeit für Adapter oder Bestellgeräte)



Bild 6-8 optiPoint 420 economy plus, optiPoint 420 economy plus S

6.3.2.3 optiPoint 420 standard, optiPoint 420 standard S

Wesentliche Merkmale

- Protokolle
  - H.323, HFA/V3 + V4, CorNet-IP, SIP
  - HTTP, DHCP, SNMP, FTP
  - H.235 (Security)
  - QoS nach DIFFSERV und IEEE 802.1 p/Q
- Sprachkomprimierung G.711, G.722, G.723 und G.729 A/B
- Power over LAN (gemäß Cisco und Standard pre802.3af)
- CTI (zum Beispiel über TAPI 1st Party)
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den LAN-Anschluss
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den PC-Anschluss
- 12 Funktionstasten mit Leuchtdioden und Self-Labeling Keys
- Grafik-Display (schwenkbar) mit 2 Zeilen zu je 24 Zeichen
- 3 Dialogtasten zur interaktiven Benutzerführung: “Ja”, “Zurück” und “Weiter”
- Vollduplex-Freisprechen mit Echo-Unterdrückung zur Raumadaption
- Anschluss für Hör-/Sprechgarnitur (121 TR 9-5)
- 2 Einstelltasten (Plus/Minus) für Lautstärke, Klangfarbe, Freisprechqualität und Display- kontrast
- Modularität:
  - 2 Adaptersteckplätze
  - 1 Schnittstelle für max. 2 Beistellgeräte
- zur Wandmontage geeignet



Bild 6-9 optiPoint 420 standard, optiPoint 420 standard S

6.3.2.4 optiPoint 420 advance, optiPoint 420 advance S

Wesentliche Merkmale

- Protokolle
  - H.323, HFA/V3 + V4, CorNet-IP, SIP
  - HTTP, DHCP, SNMP, FTP
  - H.235 (Security)
  - QoS nach DIFFSERV und IEEE 802.1 p/Q
- Sprachkomprimierung G.711, G.722, G.723 und G.729 A/B
- Power over LAN (gemäß Cisco und Standard pre802.3af)
- CTI (zum Beispiel über TAPI 1st Party)
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den LAN-Anschluss
- 1 Ethernet (10/100BaseT)-Schnittstelle (selbstkonfigurierend) für den PC-Anschluss
- 1 integrierte USB-1.1-Schnittstelle
- 18 Funktionstasten mit Leuchtdioden und Self-Labeling Keys
- Grafik-Display (schwenkbar) mit 4 Zeilen zu je 24 Zeichen
- 3 Dialogtasten zur interaktiven Benutzerführung: “Ja”, “Zurück” und “Weiter”
- Vollduplex-Freisprechen mit Echo-Unterdrückung zur Raumadaption
- Anschluss für Hör-/Sprechgarnitur (121 TR 9-5)
- 2 Einstelltasten (Plus/Minus) für Lautstärke, Klangfarbe, Freisprechqualität und Display-kontrast
- Modularität:
  - 1 Adaptersteckplatz
  - 1 Schnittstelle für max. 2 Beistellgeräte
- zur Wandmontage geeignet



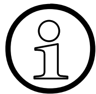
Bild 6-10 optiPoint 420 advance, optiPoint 420 advance S

6.3.3 Beistellgeräte für optiPoint 410/410 S und optiPoint 420/420 S



Vorsicht
Beistellgeräte dürfen nur bei gezogener Anschlussleitung an das Telefon angeschlossen werden.

Die Montage der Beistellgeräte erfolgt in der Regel durch den Benutzer. Die dazu erforderliche Montageanleitung befindet sich auf der CD “Elektronische Bedienungsanleitungen”.



Maximal zwei Beistellgeräte dürfen an einem optiPoint 410- oder optiPoint 420-Endgerät (nicht optiPoint 410 entry, optiPoint 410 economy, optiPoint 420 economy und optiPoint 420 economy plus) montiert werden.
Neben den beiden nachfolgend beschriebenen Beistellgeräten können auch optiPoint key module und optiPoint BLF eingesetzt werden. Tabelle 5-1 nennt die möglichen Konfigurationen von Beistellgeräten.

6.3.3.1 optiPoint self labeling key module

Das optiPoint self labeling key module ist ein seitlich am Endgerät zu montierendes Beistellgerät, das 13 zusätzliche Tasten, LED‘s und Displays für alle Zwecke bereitstellt. Self-Labeling Key bedeutet, dass jeder Taste ein Display (1 Zeile mit 12 Zeichen) zugeordnet ist, in dem die aktuell gespeicherte Funktion oder Rufnummer angezeigt wird.

Eine doppelte Tastenbelegung ist möglich.



Bild 6-11 optiPoint self labeling key module

6.3.3.2 optiPoint application module

Das optiPoint application module ist ein seitlich am Endgerät zu montierendes Beistellgerät mit Farbdisplay und integrierter alphanumerischer Tastatur. Es bietet ein persönliches Telefonbuch und andere hilfreiche Applikationen zur Verbesserung des Bedienkomforts beim Telefonieren.



Bild 6-12 optiPoint application module

Das optiPoint application module kann an folgenden Endgeräten eingesetzt werden: optiPoint 410 standard, optiPoint 410 advance, optiPoint 420 standard, optiPoint 420 advance

Im VoIP-Umfeld unterstützt dieses Beistellgerät die gleichen Funktionen wie das Vorläufermodell optiPoint 410 display module (persönliches Telefonbuch, LDAP, WAP-Browser, Java-Applikationen, Sprachwahl), jedoch mit verbesserter Ergonomie.

Das optiPoint application module muss immer als erstes Beistellgerät, dass heißt direkt am Endgerät montiert werden. Der Einsatz eines weiteren Beistellgerätes ist möglich.

Zum Betrieb des optiPoint application modules wird immer ein externes Netzgerät benötigt. Eingesetzt werden die im Abschnitt 6.6.1.2 beschriebenen Netzgeräte für optiPoint 410 und optiPoint 420. Ist ein solches Netzgerät bereits vorhanden, kann zur Speisung des optiPoint application modules der zweite Ausgang benutzt werden.

6.3.3.3 Mögliche Konfigurationen der Beistellgeräte

Die folgende Tabelle zeigt die möglichen Konfigurationen von Beistellgeräten an Endgeräten der optiPoint 410/optiPoint 410 S- und der optiPoint 420/optiPoint 420 S-Familien. Bei nicht genannten Endgeräten ist kein Einsatz von Beistellgeräten möglich.

optiPoint 410 / 410 S optiPoint 420 / 420 S	1. Beistellgerät	2. Beistellgerät
optiPoint 410 standard optiPoint 410 standard S optiPoint 410 advance optiPoint 410 advance S optiPoint 420 standard optiPoint 420 standard S optiPoint 420 advance optiPoint 420 advance S	optiPoint key module	–
	optiPoint key module	optiPoint key module
	optiPoint key module	optiPoint BLF
	optiPoint 410 display module	–
	optiPoint 410 display module	optiPoint key module
	optiPoint 410 display module	optiPoint BLF
	optiPoint 410 display module	optiPoint self labeling key module
	optiPoint BLF	–
	optiPoint self labeling key module	–
	optiPoint self labeling key module	optiPoint self labeling key module
optiPoint 410 standard optiPoint 410 advance optiPoint 420 standard optiPoint 420 advance	optiPoint application module	–
	optiPoint application module	optiPoint key module
	optiPoint application module	optiPoint BLF
	optiPoint application module	optiPoint self labeling key module

Tabelle 6-1 Beistellgerät-Konfigurationen an einem optiPoint 410/optiPoint 410 S- und optiPoint 420/optiPoint 420 S-Endgerät

6.3.3.4 Tastenprogrammierung

Die frei belegbaren Funktionstasten der optiPoint 410- und der optiPoint 420-Endgeräte, des optiPoint key modules und des optiPoint self labeling key modules können doppelt belegt werden. Dabei sind folgende Funktionsunterschiede zu beachten:

- Bis einschließlich V1.0 SMR-05:
  Eine doppelte Belegung ist möglich, wenn auf der ersten Ebene ausschließlich Rufnummern ohne LED-Unterstützung gespeichert werden. Auch auf der zweiten Ebene sind ausschließlich Rufnummern ohne LED-Unterstützung programmierbar. Dies können interne Rufnummern, externe Rufnummern und Rufnummern aus einem HiPath-Netzverbund sein.
- Ab V1.0 SMR-06:
  Mittels HiPath 3000 Manager E (*Einstellungen: Systemparameter – Flags*) oder Web-based Management WBM (*Explorer: Grundeinstellungen – System – (rechte Maustaste) System Flags*) kann eine der beiden folgenden Möglichkeiten eingestellt werden:
  – Flag "Erweiterte Tastenfunktionalität" ist nicht gesetzt (Defaulteinstellung).
    Es ergibt sich das gleiche Verhalten wie bis einschließlich V1.0 SMR-05.
  – Flag "Erweiterte Tastenfunktionalität" ist gesetzt.
    Nachdem eine beliebige Taste als "Shift-Taste" definiert wurde, können auf der dann verfügbaren zweiten Tastenebene ausschließlich Rufnummern ohne LED-Unterstützung gespeichert werden. Auf der ersten Tastenebene können beliebige Tastenfunktionen programmiert werden. Die LED-Signalisierung gilt ausschließlich für die erste Tastenebene.

Bei aktivierter Shift-Funktion leuchtet die LED der Shift-Taste. In diesem Zustand sind die Rufnummern der zweiten Tastenebene verfügbar. Mit dem Umschalten der Tastenebene wechselt bei Endgeräten mit Self-Labeling Keys auch die Beschriftung der Tasten.

Die Shift-Funktion wird nach Betätigen einer Rufnummerntaste oder nochmaligem Betätigen der Shift-Taste wieder deaktiviert.

Die Funktionstasten des optiPoint BLF's können nicht doppelt belegt werden.

6.3.4 Einsatz von optiPoint 500-Adaptern

Folgende optiPoint 500-Adapter sind für den Einsatz an Endgeräten der optiPoint 410- und der optiPoint 420-Familie (nicht optiPoint 410 entry, optiPoint 410 entry S, optiPoint 410 economy, optiPoint 410 economy S, optiPoint 420 economy, optiPoint 420 economy S, optiPoint 420 economy plus und optiPoint 420 economy plus S) freigegeben:

- acoustic adapter
- optiPoint recorder adapter

optiPoint acoustic adapter



Der optiPoint acoustic adapter dient zum Anschluss von
- einer Hör-/Sprechgarnitur (121 TR 9-5) (siehe Abschnitt 5.4.3).
- einer aktiven Lautsprecherbox und einem Beistellmikrofon über Y-Kabel.

Besetztanzeige / Türöffner und Zweitwecker / Lichtruf usw. (mit jeweils eigener Stromversorgung) über potentialfreie Kontakte (nicht unterstützt beim Einsatz des Adapters an optiPoint 410 und optiPoint 420).

Hinweise zum optiPoint acoustic adapter

- Beim Einsatz eines externen Mikrofons und eines externen Lautsprechers werden die internen Komponenten des optiPoint-Endgerätes im Freisprechmodus ausgeschaltet (sense lead).
- Die Auswahl der Freisprechbetriebsart erfolgt unabhängig davon, ob die interne oder eine externe Freisprecheinrichtung genutzt wird. Mit Ausnahme des Rufens haben externe Einrichtungen Vorrang vor internen Einrichtungen.
- Im Audiozustand Mute (Stummschaltung) wird das interne Mikrofon, die Sprechkapsel und ein am optiPoint acoustic adapter angeschlossenes Mikrofon stumm geschaltet.
- Ruf-, Alarm- und Tastentöne werden zum internen Lautsprecher und nicht zu einen am optiPoint acoustic adapter angeschlossen externen Lautsprecher übermittelt.
- Über die Lautstärketasten des optiPoint-Endgeräts wird der Lautstärkepegel des internen und eines angeschlossen externen Lautsprechers geregelt. Die Lautstärke des externen Lautsprechers kann darüber hinaus über den externen Verstärker eingestellt werden.

optiPoint recorder adapter



Der optiPoint recorder adapter ermöglicht den Anschluss eines externen Recorders oder eines Zweithörers. Achtung: Dem Gesprächsteilnehmer muss mitgeteilt werden, dass das Gespräch aufgezeichnet wird.

6.4 optiPoint 150 S

optiPoint 150 S ist das kostengünstige Einstiegsmodell für Voice-over-IP-Telefonie über das SIP (Session Initiation Protocol)-Protokoll.

Folgende Leistungsmerkmale für DSL-Telefonie-Teilnehmer werden aktiv unterstützt:

- CLIP (Anzeige der Rufnummer des rufenden Teilnehmers beim gerufenen Teilnehmer): Ausschließlich in Standalone-Systemen.
- COLP (Anzeige der Rufnummer des gerufenen Teilnehmers beim rufenden Teilnehmer)
- Rückfrage
- Halten
- Makeln
- Übergeben (Übergeben vor Melden und Übergeben nach Melden)
- DISA (Direct Inward System Access): Es können keine Leistungsmerkmale für optiPoint 150 S aktiviert werden.
- Inband DTMF: optiPoint 150 S unterstützt ausschließlich Codec G.711.

Folgende Leistungsmerkmale können DSL-Telefonie-Teilnehmer zwar nicht aktivieren, sie können allerdings passiv eingebunden werden:

- Anrufumleitung (Umleitung auf einen DSL-Telefonie-Teilnehmer wird unterstützt.)
- Konferenz (DSL-Telefonie-Teilnehmer kann passiv eingebunden werden.)
- Parken (DSL-Telefonie-Teilnehmer können geparkt werden. Aus Sicht des DSL-Telefonie-Teilnehmers ist dies wie "Halten".)
- Live Call Recording (DSL-Telefonie-Teilnehmer kann passiv eingebunden werden.)
- Automatische Berechtigungsumschaltung (DSL-Telefonie-Teilnehmer kann in automatische Berechtigungsumschaltung eingebunden werden.)
- Verkehrsbeziehungsgruppen (DSL-Telefonie-Teilnehmer kann in VBZ-Gruppen einbezogen werden.)

Folgende endgerätespezifischen Leistungsmerkmale des optiPoint 150 S werden beim Betrieb an HiPath 2000 V1.0 ab SMR-09 unterstützt:

- Anruferliste Endgerät
- Anrufschutz DND
- Gesprächsdaueranzeige
- Lokaler Rufnummernplan

- Mikrofon ein / aus
- Sprachenauswahl

Folgende Einschränkungen für DSL-Telefonie-Teilnehmer sind zu beachten:

- DSL-Telefonie-Teilnehmer sind bei HiPath 2000 V1.0 als DSS1 (funktionales Endgerät) konfiguriert und können daher nicht vom System überwacht werden (kein Monitoring). DSL-Telefonie-Teilnehmer können keine Applikationen nutzen, für die ein Monitoring erforderlich ist (zum Beispiel HiPath ComAssistant).
- Die Einbindung von DSL-Telefonie-Teilnehmern in Anrufübernahmegruppen, Sammelanschlüsse, Team-, Top- oder MULAP-Gruppen ist nicht möglich.
- DSL-Telefonie-Teilnehmer können keine Systemleistungsmerkmale aktivieren oder nutzen, die über Kennzahlen gesteuert werden können.
- Wird ein DSL-Telefonie-Teilnehmer gehalten, wird MOH eingespielt. Bei Übergabe vor Melden des DSL-Telefonie-Teilnehmers an einen anderen Teilnehmer, wird dem DSL-Telefonie-Teilnehmer kein MOH oder Rufton eingespielt.
- Wird ein geparkter DSL-Telefonie-Teilnehmer nicht von dem Teilnehmer entparkt, der ihn geparkt hat, wird das Display des DSL-Telefonie-Teilnehmers nicht aktualisiert.
- optiPoint 150 S wird nicht vom HiPath 2000-internen Deployment Service unterstützt.
- Das Makeln zwischen zwei externen Gesprächen mit dem optiPoint 150 S ist möglich. Das aktive Gespräch kann dabei durch kurzes Betätigen des Gabelumschalters getrennt werden. Ein einfaches Auflegen des optiPoint 150 S-Hörers würde die beiden externen Teilnehmer miteinander verbinden, was zu erhöhten Gesprächsgebühren führen kann. Eine solche Verbindung kann systemseitig nur durch das gezielte Trennen der Amtsleitungen oder durch ein Reset (Restart) des Systems beendet werden.
- Unter Umständen können endgerätespezifische Leistungsmerkmale an HiPath 2000 V1.0 nicht genutzt werden. Dies schließt Leistungsmerkmale ein, die über die Menüoberfläche des Endgerätes angeboten werden. Generell freigeben sind die Leistungsmerkmale, die über das Grundsystem HiPath 2000 V1.0 angeboten werden.

optiPoint 150 S



Bild 6-13 optiPoint 150 S

6.5 optiPoint 600 office

optiPoint 600 office ist ein Konvergenz-Endgerät mit $U_{P0/E}$- **und** IP-Schnittstelle (CorNet-IP). Der Betrieb an HiPath 2000 ist ausschließlich im CorNet-IP-Mode möglich.



Das auf Basis von H.323 weiterentwickelte Protokoll CorNet-IP ermöglicht, dass alle Telefonleistungsmerkmale der IP Kommunikationsplattform HiPath 2000 unterstützt werden. Somit stehen alle Telefonleistungsmerkmale wie z.B. Chef/ Sekretär, Gruppenruffunktionen, Rückruf wie gewohnt zur Verfügung. Die Bedienung, ist dabei identisch mit der Menuführung der optiPoint 500 Telefone, welche direkt an HiPath 2000 angeschlossen sind.

Spezielle digitale Signal Prozessoren (DSP) und besondere Akustik-Algorithmen (Echo Cancellation) sorgen für eine sehr gute Sprachqualität. Freisprechen und Lauthören werden somit auf einem hohen akustischen Niveau zur Verfügung gestellt.

Durch den Einsatz von Quality of Service (QoS) Protokollen sowohl auf der Ethernet Ebene wie auch IP Ebene wird ein Optimum an Sprachqualität im LAN erreicht. Die Sprachpakete des optiPoint 600 office werden mit Prioritäten-Bits versehen und somit bevorzugt vor anderen Datenpaketen durch das LAN transportiert.

Durch den eingebauten 2-Port-Ethernet-Switch kann der Arbeitsplatz PC über das optiPoint 600 office angeschlossen werden. So können Kosteneinsparungen im Bereich der Inhouse-Verkabelung und des IP Netzwerks erreicht werden.

6.5.1 Vorteile auf einen Blick

Kostensenkung

- Verkabelungskosten
  keine zusätzliche Verkabelung für
  optiPoint 600 office notwendig. Der PC wird über den integrierten Switch angeschlossen.
- Infrastrukturkosten für das Daten- und Sprachnetz
  - ein Netz,
  - ein Investment und
  - ein Team für Wartung und Service.
- Folgekosten
  Bei Umzügen/Ortsveränderungen im IP-Mode keine Konfigurationsänderung im Telefon und System

Investmentschutz

- Jeweils neuester Feature-Stand durch Software-Download

Einfache Bedienung

- Übersichtliche Anzeige durch großes
  Display und direktes Auswählen über Touchscreen Funktionalität
- Interaktive Benutzerführung über
  Dialogtasten und Display dank optiGuide
- Frei programmierbare Direktwahltasten
- Direktes Wählen aus dem PC über CTI (TAPI)

Flexibilität

- Upgrade durch Software-Download
- Administrierbar über Web-Browser und SNMP
- Schnellkonfiguration durch DHCP (plug and call)
- Anpassung an unterschiedliche Arbeitsplatzumgebungen durch Adapter und Beistellgeräte

Komfort

- Optimum an Sprachqualität im LAN durch Quality of Service (QoS)

- Spontanes Einbeziehen mehrerer Anwesender durch Freisprechen mit sehr guter Sprachqualität
- Voller Zugriff auf alle Telefonleistungsmerkmale von HiPath 2000
- Wahl direkt aus dem PC
- Großes Display mit Touchscreen Funktionalität

6.5.2 Allgemeine Lokale Leistungsmerkmale

- Kippbares graustufen Grafikdisplay mit 320*240 Punkten (8*24 Zeichen), Touch Screen Funktionalität, Hintergrundbeleuchtung und einstellbarem Kontrast
- 19 frei programmierbare Funktionstasten mit Leuchtdioden
- 3 Dialogtasten für interaktive Benutzerführung mit optiGuide
- 2 Steuertasten (Plus und Minus) zur Einstellung von Ruftonklangfarbe und Ruftonlautstärke
- Freisprechen und Lauthören
- Wahl bei aufliegendem Hörer
- Rufnummernanzeige (Calling Party Identification)
- Tasten-Klickton (key click)
- Passwortschutz für administratorrelevante Daten
- MFV-Signalisierung inband und outband
- Leistungsmerkmal-Update über Software-Download (via FTP)
- Elektronisches Notizbuch für 640 Einträge
- Kopfsprechgarnitur-Schnittstelle
  (121 TR9-5 und Polaris)
- Hearing Aid Kompatibilität
- CTI im TDM- und IP-Mode
- CAPI über USB und Callbridge for Data*
- JAVA Virtual Machine (VM) plus JAVA Development Kit (JDK) zur Generierung eigener JAVA-Anwendungen
- Virtual Key Modul (Speed Dialling Application) mit 40 Kurzwahltasten
- WAP-Bookmarks

- Eingabe von WAP-/URL-Adressen
- Resourcen-Sharing für optiPoint 600 - Einträge über die PC-Tastatur

6.5.3 Zubehör

Adapter

- optiPoint acoustic adapter
- optiPoint recorder adapter

Beistellgeräte

- optiPoint key module
- optiPoint signature module
- optiPoint BLF

6.6 Zubehör für die optiPoint-Telefonlösungen

Die folgenden Angaben gelten für die Endgerätefamilien optiPoint 410, optiPoint 410 S, optiPoint 420, optiPoint 420 S und für das Endgerät optiPoint 600 office. Auf Einschränkungen wird an den betreffenden Stellen hingewiesen.

6.6.1 Externe Netzgeräte

Beim Einsatz umfangreicher Konfigurationen oder zur Reichweitenerhöhung ist eventuell ein externes Netzgerät erforderlich.

6.6.1.1 Steckernetzgerät für optiPoint 600 office

Beim Einsatz umfangreicher Konfigurationen oder zur Reichweitenerhöhung ist eventuell ein Steckernetzgerät (SNG) erforderlich.

Über zwei MW6-Anschlußbuchsen und die mitgelieferten Verbindungskabel kann das Steckernetzgerät (Bestellnummern in Abschnitt 5.4.4) in die Anschlussleitungen eines Host- oder Client-EG’s geschaltet werden.

Technische Daten des Steckernetzgeräts AUL:06D1284:

- Netzspannung: 220 (230) V AC
- Netzfrequenz: 47 ... 53 Hz
- Ausgangsspannung: max. 50 V, min. 30 V
- Ausgangsstrom: max. 250 mA

6.6.1.2 Netzgerät für optiPoint 410/410 S und optiPoint 420/420 S

Das Netzgerät verfügt über zwei MW6-Anschlussbuchsen. Die Speisung eines Endgerätes erfolgt über die linke, mit “Digital” beschriftete Buchse.

Technische Daten

Technische Daten	Netzgerät Euro C39280-Z4-C510	Netzgerät UK C39280-Z4-C512	Netzgerät 110 V USA C39280-Z4-C511
Netzspannung	230 VAC	230 VAC	120 VAC
Netzfrequenz	50 Hz	50 Hz	60 Hz
Ausgangsspannung	max. 43 VDC, min. 30 VDC	max. 43 VDC, min. 30 VDC	max. 43 VDC, min. 30 VDC
Ausgangsstrom	480 mA	480 mA	480 mA

6.6.2 Hör-Sprechgarnituren (Headsets)

Eine Hör-/Sprechgarnitur ersetzt den Telefonhörer, das heißt der Anwender hat die Hände frei beim Telefonieren. Die Verwendung einer schnurlosen Hör-/Sprechgarnitur (121 TR 9-5) ist ebenfalls möglich.

Abschnitt 5.4.4 enthält Informationen über die verschiedenen Typen von Hör-/Sprechgarnituren und deren Bestellnummern.

Es kann eine Headset-Taste am optiPoint- oder optiset E-Endgerät eingerichtet werden, die die Rufannahme und das Umschalten zwischen Hörer (Handset) und Hör-/Sprechgarnitur (Headset) ermöglicht.



Bild 6-14 Beispiel einer schnurgebundenen und einer schnurlosen Hör-/Sprechgarnitur

Anschlussmöglchkeiten

Bei den in der folgenden Tabelle nicht enthaltenen optiPoint- und optiset E-Endgeräten ist der Anschluss einer Hör-/Sprechgarnitur nicht möglich.

Endgerät	Anschlussmöglichkeiten für schnurgebundene und schnurlose Hör-/Sprechgarnituren (Headsets)	
	direkt	über optiPoint acoustic adapter[1]
optiPoint 600 office	X	X
optiPoint 410 standard, optiPoint 410 standard S	X	X
optiPoint 410 advance, optiPoint 410 advance S	X	X
optiPoint 420 economy plus, optiPoint 420 economy plus S	X	
optiPoint 420 standard, optiPoint 420 standard S	X	X
optiPoint 420 advance, optiPoint 420 advance S	X	X

1 Die Rufannahme und das Auflegen über die Tasten der schnurlosen Hör-/Sprechgarnitur werden nur beim Anschluss über den optiPoint acoustic adapter unterstützt.

Informationen über die Vorgehensweise beim Anschluss der Hör-/Sprechgarnituren können der zum jeweiligen Lieferumfang gehörenden Installationsanleitung entnommen werden.

6.7 Bestellnummern

Eine vollständige Übersicht aller zertifizierten und lieferbaren Produkte kann der aktuellen Vertriebsinformation entnommen werden.

Artikel	Farbe	Bestellnummer
optiPoint key module	arctic	S30817-S7105-A101-*
	mangan	S30817-S7105-A107-*
optiPoint self labeling key module	arctic	xxxxx
	mangan	xxxxx
optiPoint BLF	arctic	S30817-S7107-A101-*
	mangan	S30817-S7107-A107-*
optiPoint acoustic adapter	arsen	S30817-K7110-B508-*
optiPoint recorder adapter	arsen	S30817-K7110-B408-*
Steckernetzgerät		AUL:06D1284
Steckernetzgerät UK		AUL:06D1287
Steckernetzgerät 110 V USA		AUL:51A4827
Netzgerät Euro		C39280-Z4-C510
Netzgerät UK		C39280-Z4-C512
Netzgerät 110 V USA		C39280-Z4-C511
Hör-Sprechgarnitur Encore monaural		L30460-X1282-X1
Hör-Sprechgarnitur Encore binaural		L30460-X1282-X2
Hör-Sprechgarnitur Tristar		L30460-X1282-X3
Hör-Sprechgarnitur Supra		L30460-X1282-X4
Hör-Sprechgarnitur DuoSet		L30460-X1282-X5
Hör-Sprechgarnitur Profile monaural		L30460-X1283-X1
Hör-Sprechgarnitur Profile binaural		L30460-X1283-X2
schnurlose Hör-/Sprechgarnitur		Bestellnummer liegt nicht vor.

6.8 HiPath AP 1120

Der Terminal Adapter HiPath AP 1120 verbindet bis zu zwei analoge Telefone und/oder Faxgeräte mit einem firmeneigenen oder von einem Betreiber angebotenen VoIP-Netz.

Das Gerät ist in der Lage, die gängigsten IP-Telefoniecodecs und Faxprotokolle, unter anderem auch T.38 dynamisch zu erkennen.

HiPath AP 1120 wird nur in der HFA-Variante (AP 1120 V4.0) unterstützt.



Anschlüsse

- Ethernet-Anschlüsse:
  – 1 x RJ45: 10/100 BaseT Ethernet-Zugang
  – 1 x RJ45: 10/100 BaseT Ethernet-Zugang, Stromversorgung über MDI, IEEE 802.3af (Power over LAN)
- Analoge Anschlüsse:
  – 2 x RJ11: analoges Telefon, Fax
- Stromversorgung:
  – externes 24 VDC / 12 W Steckernetzgerät
    Bei einer Spannungsversorgung über den Ethernet-Zugang (Power over LAN) wird kein Steckernetzgerät benötigt.

6.9 optiPoint WL2 professional

optiPoint WL2 professional ist das Telefon für einen unternehmensweiten einfachen Zugriff auf Daten und Ressourcen über WLAN.

WLANs sind im IP-Verkehr transparent und bilden somit die ideale Umgebung für IP-Multimedia-Anwendungen. Die Hinzunahme von Echtzeit-IP-Kommunikation, z. B. in Form von Sprache, ist ein logischer nächster Schritt, da es die Investitionen in konvergente LANs nutzt und die Reichweite der IP-Telefonie- und Multimedia-Kommunikationssysteme eines Unternehmens erweitert.

Hinweis: Aufgrund der produktspezifischen Freigabe der WLAN Access Points sind die aktuellen Informationen in der zugehörigen Freigabedokumentation zu beachten.

Das WLAN Telefon optiPoint WL2 professional (802.11) besitzt alle Features, die Wireless-Telefone heute haben müssen (z. B. polyphone Ruftonmelodien, Grafikdisplay und verschiedene Applikationen im Telefon). Zusätzlich macht das CorNet-fähige Telefon optiPoint WL2 professional die vielfältigen Telefonfeatures und Applikationen der HiPath 4000 und HiPath 3000 Systeme für Wireless-Nutzer verfügbar.

Eigenschaften

Wireless LAN Voice-over-IP Telefon mit farbigem Grafikdisplay.

Das optiPoint WL2 professional kann mit HiPath 5000 ab V5.0 benutzt werden.

- **Schnittstellen:** WLAN, USB
- **Standards:** WLAN, 802.11b (11 Mbit/s), 802.11g (volle Unterstützung von 54Mbit/s), CorNet IP, SIP

Konfiguration

- Drahtlose Verbindung mit einem WLAN-Access-Point (AP 2630 / AP 2640) als Link zu einem LAN-Switch
- IP-Verbindung zum HiPath 2000 Gateway im HiPath 3000 System; CorNet-IP-Registrierung
- IP-Verbindung zu einem SIP-Proxy/Registrar: SIP-Registrierung
- Basiskonfiguration via DHCP
- Erweiterte Konfiguration über die Telefon-Webseite (Einzeltelefon) oder Mithilfe des HiPath Deployment Service.

Leistungsmerkmale

Telefon

- Telefon mit farbigem Grafikdisplay
  (6 Zeilen, 128 x128 Pixel Auflösung, 4096 Farben, 3,1cm x 3,1cm)
- Anrufanimation und Anruferanzeige (CLIP)/Caller-ID für eingehende Anrufe
- Beleuchtetes Tastenfeld
- Zwei Softkeys zum dynamischen Zugriff auf Features
- Intuitive Benutzerführung
- Beleuchtete MWI-Taste
- Freisprechtaste
- Statusanzeige zeigt im Standby- bzw. Ruhe-Modus: Datum, Zeit, Batteriestatus, RF-Signalstärke, verbundener Access Point
- Statusanzeige zeigt während des Gesprächs: Batteriezustand, RF-Signalstärke, Gesprächszeit, abgehobener Hörer, CLIP/ Caller ID
- Anzeige der entgangenen Anrufe
- Freisprechfunktion
- Anzeige aller entgegengenommenen Anrufe
- Wählen mittels Nummerneingabe, SIP-URI (professional S) und IP-Adresse (direkter IP-Anruf)
- Mehrleitungsfunktionalität
- konfigurierbare Kurzwahltasten
- Anrufvorbereitung (Eingabe der Telefonnummern ohne Leitungsbelegung) mit Korrekturmöglichkeit
- Wahlwiederholung der letzten 10 verschiedenen gewählten Nummern
- Tastatursperre und Klingeltonabschaltung auf Knopfdruck mit Iconanzeige
- Gemeinsame Benutzeroberfläche mit Siemens Enterprise Communications GmbH & Co. KG Desktop-Telefonen über die optiGuide Benutzeroberfläche (professional S)
- Zugriff auf die HiPath-Features (abhängig vom angeschlossenen HiPath-System) für Anruf-Features wie Rückruf, Konferenzschaltung, Rückfrage etc.
- Lokale SIP-Features (professional S): Halten, Stummschaltung, Transfer, Dreierkonferenz, MWI, DND etc.

- SIP-Features mit Server-Unterstützung: Group Pickup, Priority Alerting, Distinctive Ringing, Keyset, Shared Call Appearance, Bridge Line Appearance etc.

Lokales Telefonbuch

- Umfangreiches lokales Telefon-/Adressbuch
- CLIP wird ersetzt durch den Telefonbuch- eintrag im Telefon oder im HiPath-System

Audio

- 6 polyphone Ruftöne (Lautstärke einstellbar)
- 16 Ruftöne, davon 12 vom HiPath-System verwaltet und 4 vom Nutzer verwaltet
- Ruftöne können heruntergeladen werden
- Lautstärkeeinstellung in 8 Stufen
- CLIP-/ Anrufer-ID-abhängige Ruftöne
- VIP-Anrufe

Mehrwert-Applikationen und -Features

- Sprachansage von Anrufern[1)]
  (CLIP/Anrufer-ID)
- Sprachwahl
- Polyphone Ruftöne (herunterladbar)
- Zugriff auf LDAP-Verzeichnisse
- Headset-Anschluss über einen Slim Lumberg-Stecker
- Vibrationsalarm
- Vorbereitet auf Breitband-Sprachübertragung (optional, G.722)
- CTI-Schnittstelle
- Upgrades und Konfigurationen können per Funk OTA (Over The Air) über den HiPath Deployment-Service, eine erweiterte Verwaltungsapplikation, durchgeführt werden
- Unterstützung von HiPath-Applikationen

Codecs

- G.711 (a-law und µ-law)
- G.729ab (G.729a mit VAD (Voice Activity Detection))
- G.723

- G.722 (optional)
- Advanced Echo Cancellation (AEC)

QoS*

- ToS
- DiffServ
- 802.1q
- 802.11e (WME-Subset)

Zubehör

- Tischladegerät
- Tischladegerät mit der Möglichkeit eine zweite Batterie zu laden
- USB-Datenkabel
- breite Palette an Headsets erhältlich
- verschiedene Tragehilfen sind verfügbar
- Netzadapter (passend für die jeweilige geographische Region)

Weitere Features

- WEB Browser-basierte Administration
- Mehrsprachige Benutzeroberfläche
- Datums- und Zeit-Synchronisation über NTP-Server oder HiPath-System
- Reichweite: Innerhalb von Gebäuden: bis zu 30 m (abhängig von der Umgebung)
  Im Freien: bis zu 300 m (abhängig von der Umgebung)
- Stromversorgung (Li-Ion, 3,7 V, Batterie)
- Betriebszeiten: Sprechzeit bis zu 4 h; Stand-by-Zeit bis zu 80h
- Gewicht: circa 100g
- Abmessungen:
  Telefon: 132 x 52 x 22mm (LxBxH),
  Ladegerät: 70 x 73 x 35mm
- Farbe: Light Cashmere Silver

Wireless-Features

- 802.11g (Fall-Back auf 802.11b)
- Frequenzbereich: 2,4 – 2,497 GHz
- Anzahl der wählbaren Kanäle: 13 (ETSI) oder 11 (Nordamerika)
- einstellbare Sendeleistung: ca. +20 dBm EIRP
- in das Telefon integriertes Site Survey Tool
- Datenraten: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbit/s
- SSID

Sicherheits-Features

- WEP (64, 128 Bit)
- WPA
- Cisco Infrastruktur-Support über CCX
- Telefon kann mit PIN geschützt werden
- VPN-Client
- Authentifizierung (Login/Password)
- 802.11i (optional, wenn der Standard beschlossen ist)

Authentifizierung

- EAP-TLS
- LEAP

Protokolle/Netzwerk- Features

- DHCP-Client
- FTP-Client
- VLAN-Support
- SNMP-Trap Agent
- VoIP (SIP, RTP, RTCP, TLS)
- DNS
- HTTP- und HTTPS-Server

- PPTP für VPN-Support
- UPNP (Kontrollpunkt und Gerät)
- IP-Adressierung: fixed, DHCP, PPPoE

PC-Software

- PC Tool zum Austausch von Telefonbuchdaten von Microsoft Outlook und dem lokalen Telefonbuch des WLAN Telefons
- Download von Ruftönen vom PC auf das Telefon

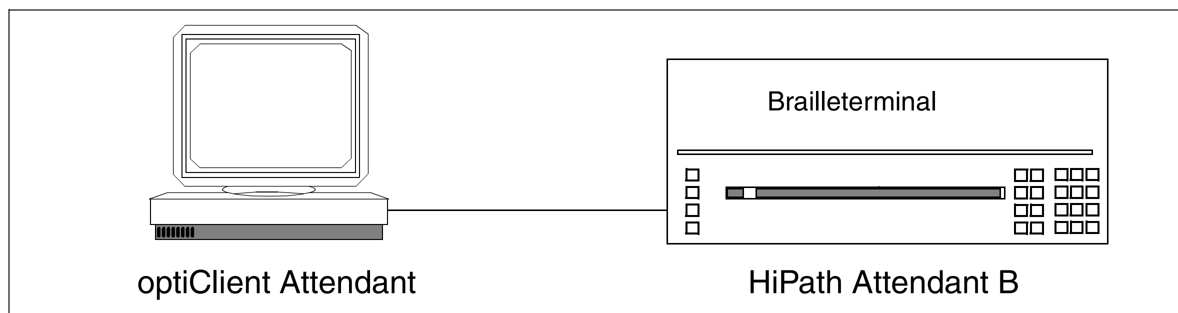
6.10 Vermittlungsplatzvarianten

6.10.1 Brailleterminal HiPath Attendant B

Definition

Für das System HiPath 2000 wird ein komfortables, anwenderfreundliches Brailleterminal als Abfrageplatz für sehbehinderte Vermittlungspersonen bereitgestellt.

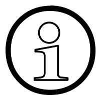
Voraussetzung für den Betrieb des HiPath Attendant B ist der PC-Vermittlungsplatz optiClient Attendant.



Auf der Braillezeile (40 Zeichen) des Brailleterminals werden die jeweils aktuellen Statusinformationen des optiClient Attendant abgebildet. Mittels Tasteneingaben steht am Brailleterminal fast die gesamte Funktionsvielfalt des optiClient Attendant zur Verfügung. Ein sehbehinderter Anwender kommt deshalb bei der Erledigung seiner Vermittlungsaufgaben einem nicht sehbehinderten Anwender sehr nahe.

Für die Einweisung des Anwenders startet nach Einschalten ein Auto-Informationsmodus, der die wichtigsten Hinweise zur Handhabung gibt. Für weitere Bedieninformation kann der Anwender einen Informationsmodus aufrufen, der ihm eine umfangreiche Bedienungsanleitung über die Braillezeile anbietet.

Das Brailleterminal passt sich der am optiClient Attendant eingestellten Sprache an. Zur Zeit sind im Brailleterminal die Sprachen deutsch und englisch implementiert. Weitere Sprachen sind in Vorbereitung.



Das Brailleterminal Attendant B ist direkt bestellbar bei:
Winkler Kommunikationstechnik
Ahornstrasse 12
26180 Rastede / Ipwege
Deutschland
Tel.: ++49-4402-929292
Fax: ++49-4402-929294
http://www.juergen-Winkler.com
Bestellbezeichnung: BT-H150 Office-PCVF-001-A
Die Lieferzeit beträgt ca. 6 Wochen nach Bestelleingang.

6.10.2 optiClient Attendant (Version 7.0)

Einleitung

Der optiClient Attendant ist ein PC-basierter Vermittlungsplatz (PC-VPL) für HiPath 2000, der einmal pro System eingesetzt werden kann.

Darüber hinaus kann der optiClient Attendant als zentraler Vermittlungsplatz in einem HiPath-Netzverbund betrieben werden.

HiPath 2000 V1.0 unterstützt den optiClient Attendant ab Version 7.0. Der Einsatz früherer Versionen des optiClient Attendant ist nicht möglich.

Anschaltevarianten

1. Anschaltung per TCP/IP
2. Anschaltung über USB-Schnittstelle des optiPoint 600

Leistungsmerkmale des optiClient Attendant V7.0

- Anzeige der wartenden Gespräche mit Typ, Name und Rufnummer
- Akustische Signalisierung mit Lautstärkeregelung
- Anzeige des Vermittlungszustandes von Quelle und Ziel
- Abfrage von anstehenden Gesprächen
- Auswahl von Telefonbüchern:
  - Outlook Kontakte,
  - HiPath-Telefonbuch,
  - Attendant-Internes Telefonbuch auf Microsoft Access Datenbasis,
  - LDAP auf Microsoft Active Directory Server,
  - Zugriff auf Telefonbuch-CD.
- Notizbuchfunktion um Rufnummern zu speichern und zu wählen
- Anrufstatistik für kommende Rufe mit Sortierfunktion nach verschiedenen Kriterien
- Komfortable Anruferliste mit nahezu unbegrenzter Anzahl von Einträgen, sortiert nach Datum und Uhrzeit
- Zusatzfunktionen wie Haltetasten, Aufschalten, Rückruf, Konferenz, Personensuche, Lautsprecherdurchsagen, Alarmsignalisierung, Gebührenabfrage, Wahlwiederholung (10 letztgewählte Ziele)

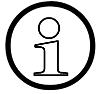
- Onlinehilfe unter Windows
- Komfortable Konfiguration einzelner Leistungsmerkmale,
- Servicetools für Diagnose und Protokolle
- Einfaches Installationsprogramm
- Benutzeroberfläche z. Zt. in Deutsch, Englisch, Niederländisch, Portugiesisch, Italienisch, Französisch und Spanisch vorhanden
- Verbinden mit Gebühren für Einzelgespräche mit automatischer Anzeige im Notizbuch (ausdruckbar).
- Anschaltung eines Blindenterminal optional.
- Besetztlampenfelder bieten:
  - Je Besetztlampenfeld mit 140 Namen á 16 Zeichen oder 240 Rufnummern á 6 Zeichen
  - Anzeige von bis zu drei Besetztlampenfeldern möglich,
  - Anschaltung eines zweiten Bildschirms optional
  - Individuelle Anpassung der Besetztlampenfelder durch den Benutzer
  - Zoomen des BLF mit automatischer Anpassung der Schriftgröße
  - Schnellwahl über Besetztlampenfeld
  - Farbliche Anzeige der Teilnehmerzustände frei, wird gerufen, intern belegt, extern belegt, umgeleitet, Anrufschutz
  - Erfassen einer Notiz je BLF-Teilnehmer als Eigeninformation für den Benutzer
  - Erfassen von bis zu 2 Vertretern je BLF-Teilnehmer mit Wahlfunktion
  - Sortieren des BLF bzw. von Teilen des BLF nach Rufnummer oder Alphabet
  - Namensdefinition für Besetztlampenfelder
  - Definition von Überschriften für Gruppen von BLF-Teilnehmern

Anschaltevarianten in Abhängigkeit vom Microsoft Betriebssystem

Anschaltevariante	Windows®2000	Windows®XP
integrierte USB-Schnittstelle (optiPoint 600 office)	Ja	Ja
TCP/IP	Ja	Ja

Zusätzliche Microsoft Betriebssysteme werden nicht unterstützt.

Systemvoraussetzungen



Falls die Lizenzierungskomponenten Customer License Agent CLA und Customer License Manager CLM auf dem gleichen PC installiert werden sollen, sind deren Systemvoraussetzungen zusätzlich zu berücksichtigen.

- Pentium III ab 750 MHz
- mind. 128 MB RAM (Arbeitsspeicher)
- Grafikauflösung mind. 1024 x 768 Pixel
- Soundkarte mit Lautsprecher für die Anrufsignalisierung.
  Bei Windows®2000 muss zur Signalisierung über die Soundkarte folgende Konfiguration vorgenommen werden: Wählen Sie `Start/Einstellungen/Systemsteuerung/Sounds und Multimedia/Sounds` und aktivieren Sie "Nur bevorzugte Geräte verwenden".
- Microsoft kompatible Maus
- CD-ROM- oder DVD-Laufwerk
- mind. 40 MB freier Festplattenspeicher
- Betriebssystem Windows®2000 oder Windows®XP
- Beim Betrieb mit TCP/IP-Anbindung: Betriebsbereites Betriebssystem mit konfigurierter Netzwerk- und Soundkarte.
- Beim Betrieb an USB: optiPoint 600 office mit freier USB-Schnittstelle, USB-Kabel (Sachnummer S30267-Z360-A30-1), USB-Treiber (in Software Call-Bridge-TU enthalten) und einen freien USB-Anschluss am PC.

Lizenzierung

Der optiClient Attendant V7.0 ist lizenzierungspflichtig. Die Lizenzierung erfolgt über das System HiPath 2000.

6.10.3 optiPoint Attendant

Vermittlungsdienste können bei der HiPath 2000 mit einem speziell eingerichteten Telefon ausgeführt werden. Dieser optiPoint Attendant (VPL) dient gleichzeitig als Abwurfplatz. Am VPL laufen alle Gespräche auf, wenn keine Durchwahlmöglichkeit besteht, oder wenn über die Rufzuordnungsalgorithmen im Call Management kein Teilnehmer erreicht werden konnte (Abwurf). Die Vermittlungsperson leitet dann die kommenden Gespräche zu den gewünschten Teilnehmern weiter.

Eine Einrichtung als optiPoint Attendant ist für folgende Endgeräte möglich: optiPoint 410 economy/economy plus/standard/advance, optiPoint 420 economy/economy plus/standard/advance und optiPoint 600 office.

Die Funktionstasten des für optiPoint Attendant verwendeten Systemtelefons sind wie folgt vorbelegt und können - falls nötig - vom Servicetechniker geändert werden:

- Nachtschaltung (Ein-/ausschalten der Nachtschaltung)
- Telefonbuch (Öffnen des internen Telefonbuchs)
- wartende Anrufe (gibt Auskunft über die Anzahl der wartenden Anrufe)
- Aufschalten (eintreten in eine besetzte Verbindung)
- Halten (Halten eines Gesprächsteilnehmers)
- Extern 1 (erstes externes Gespräch, kommend/gehend)
- Extern 2 (zweites externes Gespräch, kommend/gehend)
- Trennen (Trennen oder Verbinden eines Gesprächs)

optiPoint Attendant kann entsprechend den individuellen Bedürfnissen des Kunden mit key modules und / oder mit Besetztlampenfeldern (optiPoint BLF) ausgestattet werden. Dadurch wird die Anzahl der Funktionstasten (speziell der internen Namentasten) erweitert (siehe Tabelle).

Tasten gesamt	**16**	**32**	**48**	**64**	**90**	**106**	**122**	**180**	**196**	**212**
Anzahl key modules	1	2	3	4	–	1	2	–	1	2
Tasten key modules	16	32	48	64	–	16	32	–	16	32
Anzahl BLF’s (optiPoint BLF)	–	–	–	–	1	1	1	2	2	2
Tasten BLF’s (optiPoint BLF)	–	–	–	–	90	90	90	180	180	180

Tabelle 6-2 optiPoint Attendant - Summe der Funktionstasten durch weitere key modules und BLF’s

Beim Anschluss von insgesamt 2 key modules und 2 optiPoint BLF’s können max. 212 interne Namentasten (mit interner Teilnehmer-Rufnummer) mit Besetztanzeige dargestellt werden.

6.11 Analoge Workpoints für HiPath 2030

HiPath 2030 ist mit zwei a/b-Schnittstellen (RJ45-Buchsen) für den Anschluss von analogen Endgeräten (zum Beispiel Fax Gruppe 3) ausgestattet. Die Schnittstellen liefern eine Rufspannung von 45 V_{eff}.

6.12 ISDN-Workpoints

Die S_0-Schnittstellen können optional als ISDN-Teilnehmerschnittstellen konfiguriert werden. Anzuschließende Endgeräte müssen über eine eigene Speisung verfügen (zum Beispiel über ein Steckernetzgerät).

Die Aktivierung von LM's ist bei den S_0-Endgeräten typabhängig. Je nach verwendetem Endgerät werden verschiedene ISDN-Leistungsmerkmale unterstützt. Darüber hinaus ist die Aktivierung von Systemleistungsmerkmalen über die Kennzahlprozeduren für analoge Teilnehmer möglich. Es werden nur Systemleistungsmerkmale unterstützt, die im Ruhezustand des Endgeräts aktivierbar sind.

Das Wahlverhalten von ISDN-Endgeräten entspricht dem von IWV-Endgeräten. Für die im ISDN-Protokoll nicht nutzbaren Zeichen "*" und "#" können die Ersatzkennziffern "75" und "76" verwendet werden.

7 Applikationen

7.1 Übersicht

Der Leistungsumfang des Systems HiPath 2000 kann durch den Anschluss von Applikationen erweitert werden. Dazu zählen Produkte für die Automatische Anrufverteilung (ACD), Hotelapplikationen, Voice Messaging-Dienste, Gebührencomputing und Mobilkommunikation.

HiPath 2000 unterstützt CSTA Phase I (Einzelplatzlösung) und CSTA Phase III (Zentrale Client / Server-Lösung).

7.2 Liste der zertifizierten Applikationen

Applikation		**HiPath 2020**	**HiPath 2030**
Name	**Version**		
Mobile Office			
HiPath ComAssistant V1.0	V1.0	X	X
HiPath Xpressions (HiPath Xpressions V3.0 / HiPath Xpressions V4.0)	V3.0/V4.0	X	X
HiPath SimplyPhone for Outlook V3.1 und HiPath SimplyPhone for Notes V3.1 und V4.0	V3.1/4.0	X	X
Management Applikationen			
HiPath Fault Management V3.0	V3.0	X	X
TeleData Office V3.0	V3.0	X	X
Middleware			
HiPath TAPI 120 V2.0	V2.0	X	X
CAP TAPI Service Provider	V3.0	X	X

7.3 HiPath ComAssistant V1.0

ComAssistant ist eine serverbasierte CTI-Lösung fürs Intranet. Software-Installation und Konfiguration erfolgt zentral auf dem Server. Auch die benutzerbezogenen Journaldaten und Einstellungen werden auf diesem Server gespeichert. Dadurch entfallen Clientinstallationen völlig. Eine schnelle und einfache Verbreitung im Intranet ist damit sichergestellt.

Da die Funktionalität über HTML-Seiten und HTTP-Requests angeboten wird, genügt ein Web-Browser, um ComAssistant von jedem Rechner im Intranet sofort nutzen zu können.

Auch wenn der PC des Anwenders ausgeschaltet ist, werden alle für ihn relevanten Journalinformationen auf dem Server weitergeführt.

Die Sicherung der Benutzerdaten erfolgt zentral.

Neben der wichtigen Möglichkeit, die Telefonie-Funktionalität in eigene Web-Seiten mittels HTTP-Requests zu integrieren, wird mit ComAssistant eine Standard Benutzeroberfläche ausgeliefert, über die alle Funktionen genutzt werden können.

ComAssistant Rules ist die ComAssistant-Komponente, die die Regeldefinition und Interpretation übernimmt.

Der ComAssistant Rules erweitert die Funktionalität von ComAssistant CTI, Exchange (Outlook) oder Lotus Notes/Domino um Regeln/Regelsätze zur Anrufumleitung bzw. Weiterleitung von E-Mails und bietet eine komfortable Sprachanbindung.

Der ComAssistant Rules ermöglicht Ihnen unter anderem eine Anrufumleitung - je nach Wichtigkeit des Anrufers - entweder auf das Sprachinfo-System oder das Mobiltelefon, passend zu einem bestimmten Termineintrag.

Der ComAssistant besteht aus vier Komponenten:

- **ComAssistant CTI**
  HiPath ComAssistant CTI ist eine servergestützte Anwendung, die Telefonie-Funktionalität Web-basiert im Intranet zur Verfügung stellt. HiPath ComAssistant CTI ist ideal geeignet für die Integration von CTI in bereits existierende Intranet-Lösungen.
- **ComAssistant Rules**
  Der ComAssistant erweitert die Funktionalität von ComAssistant CTI, Exchange (Outlook) oder Lotus Notes/Domino um Regeln/Regelsätze zur Anrufumleitung bzw. Weiterleitung von E-Mails und bietet eine komfortable Sprachanbindung.
- **ComAssistant DB**
  ist die Datenbank des ComAssistant. Sie wird als Bestandteil von ComAssistant Rules installiert und ist die Basis für alle benutzerbezogenen Daten.

- **ComAssistant Group**
  ist die Groupwarekomponente des ComAssistant.
  Diese Zusatzkomponente stellt Anbindungen für Lotus und Exchange zur Verfügung. Sie muss auf dem Groupware-Rechner installiert werden und auf dem Lotus- bzw. Exchange-Server laufen.

7.4 HiPath Xpressions (HiPath Xpressions V3.0 / HiPath Xpressions V4.0)

HiPath Xpressions unterstützt den Anwender beim täglichen Austausch von Sprach-, Fax- und E-Mail-Informationen.

Dabei spielt es prinzipiell keine Rolle, wo sich der Anwender gerade befindet. Durch den flexiblen Zugriff über Telefon oder PC kann im Büro, von zu Hause (z. B. als Teleworker) oder von unterwegs (auf Dienstreisen, beim Kunden, usw.) auf **HiPath Xpressions** zugegriffen werden. Personengruppen, die vorwiegend mit dem Mobiltelefon kommunizieren, können mittels Short Message Service (SMS) über neue Nachrichten informiert werden, sich SMS-Nachrichten an das Mobiltelefon senden lassen und auf sämtliche Sprach-, Fax- und E-Mail-Nachrichten zugreifen. **HiPath Xpressions** bietet somit für alle Anwendergruppen im Unternehmen eine flexible Lösung.

HiPath Xpressions vereint die Dienste

- Voice-Mail,
- Fax-Mail,
- E-Mail und
- SMS

auf einer Windows2000/2003-Plattform zu einem Unified Messaging System. Dank seiner modularen, skalierbaren Client/Server-Architektur erlaubt diese Lösung eine optimale Anpassung an den individuellen Kommunikationsbedarf unserer Kunden. Offene Standards, Integration in bestehende DV- und TK-Umgebungen, universeller Zugriff auf Nachrichten per PC und Telefon, und der gesicherte Zugang via ISDN, LAN und Intranet/Internet garantieren bereits heute Investitionssicherheit für die Zukunft. Sie können bedarfsgerecht Dienste, Userpakete, DV-Integrationen sowie software-only Lösungen auswählen. Damit kann von der kleinen Einstiegsvariante bis hin zu vernetzten Kommunikationslösungen für jeden Anspruch die maßgeschneiderte Lösung geliefert werden.

HiPath Xpressions ist mobil und macht mobil. So kann zum Beispiel für jeden Ihrer Mitarbeiter eine eigene Mailbox eingerichtet werden. Liegt eine Nachricht vor, wird diese nicht nur am PC signalisiert, sondern auf Wunsch an jedem beliebigen Telefon am Arbeitsplatz oder Mobiltelefon. Die Nachricht kann am PC im Büro, zu Hause oder im Hotel abgerufen werden. Auch das Home Office funktioniert dann reibungslos, wenn der Teleworker jederzeit Zugriff auf die Unternehmensressourcen hat. Kein Problem mit **HiPath Xpressions**.

Mit dem Zusatzleistungsmerkmal Fax-on-Demand können Ihre Kunden rund um die Uhr Informationen, wie aktuelle Preise, Produktdaten, Marktprognosen oder Wettervorhersagen, abrufen. Ein Service, mit dem clevere Unternehmen Geld sparen oder sogar verdienen.

Unified Messaging

Unified Messaging bedeutet die Integration der Dienste Voice-, Fax-, E-Mail und SMS. In einer teilnehmerbezogenen Mailbox stehen alle persönlichen Nachrichten zum Abruf bereit. Die internetorientierte Funktionalität ermöglicht Ihnen am PC den Zugriff mit allen IMAP4-Clients (z. B. Netscape Communicator oder Outlook Outlook 2000/XP/2003). Somit müssen Sie nicht auf Ihre gewohnte Benutzeroberfläche verzichten. Unterwegs steuern Sie Ihre Mailbox ganz einfach mit dem Telefon.

Besonders attraktiv ist Unified Messaging für Unternehmen, die bislang über kein E-Mail System verfügen. Sie sparen diese separate Investition ohne auf eine leistungs- und internetfähige E-Mail Komponente zu verzichten.

Die Dienste sind zudem einfach in Ihre vorhandene Kommunikationslandschaft zu integrieren. Optimierte Versionen sind für MS Exchange, Lotus Notes und SAP R/3 verfügbar (siehe DV-Integrationen).

Fax-Mail und Fax-Applikationen

Jeder Teilnehmer besitzt ein persönliches diensteübergreifendes Postfach mit eigener Durchwahlnummer für das Versenden und Empfangen von Fax-Nachrichten. Dieses Postfach ist vor unbefugten Zugriffen durch Passwort geschützt.

Fax empfangen
Fax-Nachrichten, die an die Fax-Rufnummer eines Teilnehmers adressiert sind, werden in dessen Postfach gespeichert und stehen somit zum Abruf bzw. Weiterverarbeiten bereit.

Automatische Faxtonerkennung
Ist die Anrufumleitung am Arbeitsplatztelefon aktiv, wird entsprechend der typischen Funktionalität analoger Telefon/Fax-Kombigeräte der Anruf auf Dienst Fax von **HiPath Xpressions** geprüft und ggf. auf die Annahme einer Fax-Nachricht umgeschaltet.

Vertretungsregelung
Jede empfangene Nachricht kann automatisch an einen anderen Teilnehmer weitergeleitet werden, um zu gewährleisten, dass (z. B. im Urlaub) keine Nachricht unbearbeitet bleibt.

Fax-Viewer/-Editor
Empfangene Fax-Nachrichten können mittels eines Standard Fax-Viewers/-Editor für TIFF- oder JPEG-Format am PC dargestellt und weiterverarbeitet werden, bzw. ist mit **HiPath Xpressions** Extension für MS Outlook 2000/XP/2003 integriert.

Ausgabe auf LAN-Drucker
Empfangene Fax-Nachrichten müssen nicht zwingend auf einem Fax-Gerät, sondern können jederzeit auf einem LAN-Drucker ausgegeben werden. Die Anzahl der benötigten Faxgeräte im Unternehmen kann dadurch deutlich reduziert werden.

Ausgabe von E-Mails als Fax
Empfangene E-Mails können incl. konvertierbarer Attachments als Fax auf einem beliebigen Faxgerät ausgegeben werden. Damit bleiben Sie auch unterwegs immer informiert.

Archivierung

Bei eingehenden Fax-Nachrichten mit z. B. unternehmenswichtigen Daten werden diese nicht nur an den Original-Empfänger gesendet, sondern kann zusätzlich eine Kopie dieser Mitteilungen in einer separaten Mailbox (z. B. zum Zwecke der zentralen Archivierung mit einer externen Anwendung) abgelegt werden.

Fax senden

- **Faxdeckblatt und –logo**
  Beim Versand können teilnehmerindividuell Faxdeckblatt und –logo eingesetzt werden.
- **Fragmentierter Faxversand**
  Bei einer Unterbrechung während des Sendevorgangs wird die Übertragung bei der Seite fortgesetzt, an der sie zuvor unterbrochen wurde. Die Fortsetzung des Versendevorgangs kann durch einen konfigurierbaren Vermerk gekennzeichnet werden.
- **Senden aus einer MS-Office-Applikation**
  Fax-Nachrichten können direkt aus einer MS Office-Applikation (z. B. MS Word für Windows, MS PowerPoint, etc.) generiert und versandt werden.
- **Zeitversetztes Senden**
  Anhand der Prioritätsstufen normal, mittel, und hoch kann der Anwender den Zeitraum für die Versendung des Faxes bestimmen. Die Zeiträume werden zentral, für alle Anwender gleich, den Prioritäten zugewiesen.

Fax on Demand
Im **HiPath Xpressions** hinterlegte Fax-Dokumente stehen je nach Bedarf zum Abruf bereit. Jedem dieser bereitgestellten Dokumente ist eine Rufnummer fest zugeordnet. Durch das Anwählen dieser Rufnummer von einem Fax-Gerät aus wird das Dokument übermittelt. Bei dieser Art von Übertragung trägt der Anrufer die Verbindungskosten.

Voice-Mail

Die Voice-Mail-Anwendung des **HiPath Xpressions** bietet jedem Benutzer die Möglichkeit, Sprachnachrichten zu empfangen, zu speichern, weiterzuleiten, diese zu beantworten und zu kommentieren. Diese Oberfläche steht vom Telefon oder PC zur Verfügung. Auch Fax- und E-Mail-Nachrichten können über Voice-Mail ausgegeben werden. Faxe können z. B. auf einen Drucker weitergeleitet oder an ein beliebiges Faxgerät gesendet werden. Bei E-Mails besteht die Möglichkeit, dass sie vorgelesen werden (Text to Speech).

Bedienerführung
Eine akustische Bedienerführung unterstützt Sie bei allen Funktionen. Ausführliche, zusätzliche Informationen können Sie über die Hilfe-Funktion abrufen. Bei der Verwendung eines di-

gitalen Endgeräts an der Hicom 300 E/ 300/ 300 H oder HiPath 4000 werden Sie zusätzlich zur gesprochenen Bedienerführung über die einzelnen Schritte auch im Display informiert. Bei den genannten Funktionen je Teilnehmer haben Sie die Wahl zwischen einer deutschen, UK- oder US-englischen, französischen, kanadisch-französischen, italienischen, portugiesischen, brasilianisch portugiesischen, spanischen, amerikanisch spanischen, türkischen, russischen oder niederländischen Bedienerführung. Die Bedienerführung steht in diesen Sprachen mit einer Hicom PhoneMail oder einer Hicom 300 VMS vergleichbaren Bedienoberfläche zur Verfügung. Jeder Teilnehmer kann sich seine Bedienoberfläche über seine Administrationsebene einstellen, wenn diese im System zur Verfügung gestellt wird.

Für externe und interne Anrufer
Sie haben die Möglichkeit, bei Abwesenheit (Besprechung, Dienstreise, Urlaub, usw.) Anrufe zu ihrer Mailbox umzuleiten. Ein Anrufer hört Ihre persönliche Ansage und nach einem Signalton kann er eine Nachricht für Sie hinterlassen. Dieses gilt auch für den Fall, dass die Postfachgrenzen des Teilnehmers erreicht wurden. Möchte der Anrufer keine Nachricht hinterlegen, sondern direkt mit einem Teilnehmer sprechen, so kann er eine Telefonverbindung zu einer Vertretung oder zur Vermittlung herstellen, ohne erneut anrufen zu müssen.

Für Mailboxinhaber
Nach Eingabe der Zugriffsnummer auf **HiPath Xpressions** schließt sich eine Ansage zur Bedienerführung an. Zum Ausgeben vorliegender Nachrichten (Voice, Fax, E-Mail), zum Senden von Nachrichten usw. ist die Eingabe der persönlichen Rufnummer und eines Passwortes erforderlich.

Passwort
Alle gespeicherten Nachrichten sind durch ein Passwort geschützt. Dieses kann vom Benutzer jederzeit geändert werden. Wird das Passwort wiederholt falsch eingegeben, unterbricht **HiPath Xpressions** die Verbindung und stellt bei externen Anrufern eine Verbindung zur Vermittlung her.

Nachrichten empfangen
Sie legen fest, ob der Anrufer bei Abwesenheit nur einen Hinweistext hören (Hinweisfunktion) oder nach der Ansage eine Nachricht hinterlassen kann (Anruferbeantworterfunktion).

Optische und akustische Signalisierung
Der Hinweis auf eine eingetroffene Nachricht erfolgt bei digitalen Endgeräten mit Display optisch durch das Leuchten der Briefkastenlampe und beim Abheben des Hörers durch eine Ansage. Nach Drücken der Briefkastentaste erfolgt im Display des digitalen Telefons an Hicom 300 E / 300 / HiPath 4000 der Hinweis auf eine vorliegende Nachricht im **HiPath Xpressions**.

Bei analogen und digitalen Telefonen ohne Display erhalten Sie nur einen akustischen Hinweis. Über den Standardzugriff auf die eigene Mailbox können Nachrichten abgerufen werden.

Benachrichtigungsdienst
Bei neu vorliegenden Nachrichten können Sie sich per SMS informieren lassen. Jeder Teilnehmer kann dies dienstebezogen frei konfigurieren. Somit erhalten Sie je nach Bedarf für Voice-Mail, Fax-Mail und E-Mail eine Kurznachricht auf Ihrem Mobiltelefon. Diese Einstellungen sind jederzeit vom Telefon oder komfortabel mit dem Web Administration Client änderbar.

Nachrichten anhören
Durch Anwählen Ihrer Mailbox können Sie ortsunabhängig und jederzeit gespeicherte Nachrichten am Telefon anhören. Innerhalb einer Nachricht können Sie dabei vorwärts und rückwärts springen oder eine Pause einlegen.

HiPath Xpressions unterscheidet sowohl die unterschiedlichen Dienste wie

- Voice-Mail
- Fax-Mail
- E-Mail

als auch folgende sogenannte Nachrichtenwarteschlangen:

- Empfangene Nachrichten bzw. solche, die nicht zugestellt werden konnten.
- neue Nachrichten,
- bereits abgehörte Nachrichten,
- Nachrichten, die nach Abschluss der Verbindung mit **HiPath Xpressions** versendet werden.

Bei mehreren Nachrichten können Sie vorwärts und rückwärts blättern, um gezielt eine Nachricht zu suchen.
In Ihrem **HiPath Xpressions**-Postfach auf Ihrem PC können Sie Ihre Sprachnachricht selektieren und auch z. B. über den eingebauten Lautsprecher ausgeben.

Nachrichten beantworten/weiterleiten

Nach Anhören einer vorliegenden Nachricht können Sie diese löschen, speichern oder bearbeiten. So können Sie z. B. die Antwort auf die Frage eines internen Teilnehmers auf dessen Mailbox sprechen, ohne seine Rufnummer erneut anwählen zu müssen oder eine direkte Verbindung zu dem internen oder externen Absender herstellen. Die Nachricht kann auch mit einem Kommentar an andere Mailboxinhaber weitergeleitet werden. Kommentierte Nachrichten können wiederum kommentiert weitergegeben werden.

Diese Funktionalität steht Ihnen vom Telefon und PC zur Verfügung.

Nachrichten versenden

- an einen Empfänger
  Sie können eine gesprochene Nachricht zur Mailbox eines anderen Benutzers weiterleiten. Dies ist von jedem Ort und rund um die Uhr möglich.

- an Verteiler
  Zum Senden von Nachrichten an einen bestimmten Empfängerkreis können Sie sich an Ihrem PC persönliche Verteiler einrichten. Jeder Verteiler kann dabei bis zu 99 Rufnummern enthalten. Ebenso können für alle Mailboxinhaber zentrale Verteiler eingerichtet werden.

Nachrichten erstellen
Eine Sprachnachricht kann nicht nur am Telefon, sondern auch am PC aufgenommen und versendet werden.

Persönliche Ansagen/Zentrale Ansagen

- Persönliche Ansage (Begrüßung)
  Jeder Mailboxinhaber kann seine persönliche Namensansage aufsprechen ansonsten wird standardmäßig die Rufnummer des gewählten Teilnehmers ausgegeben.
  Ergänzend können Sie zwischen neun persönlichen Ansagetexten wählen. Diese persönlichen Ansagetexte kann der Benutzer zeitabhängig folgenden Anrufsituationen zuordnen:
  - Alternativansage (Verwendung für interne und externe Anrufer)
  - Ansage für interne Anrufer
  - Ansage für externe Anrufer
  - Ansage bei besetzt

Wenn Sie keine persönliche Ansage
aktiviert haben, wird standardmäßig die Systemansage genutzt und der Anrufer kann danach seine Nachricht hinterlassen.

- Zentrale Ansage
  Neben den persönlichen Begrüßungsansagen können zentrale Ansagen eingerichtet werden, die für alle Benutzer Gültigkeit haben.

Automatischer Vermittlungsplatz

Zur Verbesserung der Kundenerreichbarkeit steht die Funktion Automated Attendant zur Verfügung. Nach erfolgter Begrüßung und Angabe einer Optionsauswahl kann ein Anrufer sich entweder tiefergehende Ansprechpartner selektieren, direkt eine Telefonverbindung zum selektierten Ansprechpartner herstellen oder sich automatisch mit der Vermittlung verbinden lassen.

7.5 HiPath SimplyPhone for Outlook V3.1 und HiPath SimplyPhone for Notes V3.1 und V4.0

HiPath SimplyPhone ist ideal geeignet für Arbeitsplätze, die Lotus Notes oder Outlook 98 als universelles Kommunikations- und Organisationstool nutzen.

Telefongespräche können im Lotus Notes Dokumenten gespeichert werden. Bei eingehenden Anrufen werden die Gesprächspartner in den Lotus Notes / Domino-Adressbüchern oder globalen LDAP-Adressbüchern (MetaDirectory) erkannt.

Von Einträgen aus Lotus Notes Ansichten, persönlichen Adressbüchern und Domino-Verzeichnissen, Journal und E-Mail-Datenbanken kann per Menüeintrag direkt telefoniert werden. Eine Teilnehmersuche im persönlichen Adressbuch, Domino-Verzeichnis und globalen LDAP-Adressbüchern (MetaDirectory) und anschließende Wahl aus der Ergebnisliste ist ebenfalls möglich.

HiPath SimplyPhone for Lotus Notes 3.1 ist ein CTI Client, der auf der Microsoft-Telefonieschnittstelle TAPI basiert und mit verschiedenen TAPI Service Providern genutzt werden. kann.

HiPath SimplyPhone for Lotus Notes 3.1 erweitert den vorhandenen Funktionsumfang von Microsoft Outlook 2000 oder 98 um komfortable Telefoniefunktionen wie Rückfrage, Konferenz, Rufweiterschaltung und Makeln, Anrufumleitung sowie die folgenden CTI-Leistungsmerkmale:

- Anrufen von Einträgen aus Lotus Notes Ansichten und persönlichen Adressbüchern und Domino-Verzeichnissen, Journal und E-Mail-Datenbanken
- Anruferidentifizierung aus Lotus Notes privaten Adressbüchern und Domino-Verzeichnissen oder globalen LDAP-Adressbüchern (MetaDirectory).
- Protokollierung der Anrufe in Lotus Notes Dokumenten
- Anrufplanung und Rückrufliste in Lotus Notes Mail/Journal-Datenbank. E-Mail-Benachrichtigung bei umgeleiteten oder übernommenen Anrufen.

7.6 HiPath Fault Management V3.0

Mit **HiPath FM** werden die primären Forderungen nach einer ausfallsicheren Kommunikation in idealer Weise unterstützt.

Unabhängig davon:

- ob es sich um Sprach- oder Datenkommunikation handelt,
- über welche Infrastruktur kommuniziert wird, über Leitung, LAN oder wireless,
- ob Terminals, Systeme, Server oder komplexe Lösungen wie Call Center und andere Applikationen überwacht werden sollen,
- ob es sich um kleine Netze oder eine länderübergreifende Netztopologie mit mehreren hundert Einzelsystemen in verschiedenen Netzdomänen handelt.

HiPath FM signalisiert bereits erste Anzeichen einer Störung in einem übersichtlichen grafischen Netzspiegel, mit Priorität und Ort des Fehlers. Mit einer Vielzahl von weiteren Informationen, die zur umgehenden Fehlerbehebung beitragen. Und dies noch lange bevor die Netz-Teilnehmer Störungsauswirkungen bemerken.

HiPath FM erlaubt die Überwachung der Kommunikationsressourcen auch ohne umfangreiches Expertenwissen durch einfache grafische Bedienoberfläche und umfangreiche Supportfunktionen.

HiPath FM ist in Java programmiert, womit der Einsatz auf nahezu allen gängigen Betriebssystemen und Rechnerplattformen ermöglicht wird. Mobilität wird dem Anwender durch Internet-Zugang mit Web-Browser geboten.

HiPath FM trägt damit ganz wesentlich dazu bei, dass ein sicherer Betrieb des Kommunikationsnetzes gewährleistet ist und die Wettbewerbsfähigkeit Ihres Unternehmens erhalten bleibt.

HiPath FM ist über Gateways der Firma Materna GmbH sowohl in die Umbrella Management Systeme HP OpenView und IBM Tivoli NetView integrierbar, als auch in das Prozess Management System „Action Request"

Systemfunktionen

Client-Server-Architektur
Der Server verwaltet sämtliche Informationen, sowie die angemeldeten Clients. Er überwacht die Zugriffe auf die Managed Objects. Der Client stellt die im Server verwalteten Informationen grafisch dar.

Client Access
Der Zugang zum HiPath FM-Client ist sowohl als Java-Einzelplatzanwendung als auch mit Web-Browser möglich. Dadurch ist die Anwendung von nahezu jedem Ort aus betreibbar.

Single Point of Access (SpoA)
Ermöglicht den Zugang zu weiteren Applikationen der einzelnen Element Manager, um z. B. Konfigurationsänderungen in den Kommunikationssystemen vorzunehmen.

Plattformunabhängigkeit
Die auf Java basierte SW des HiPath FM erlaubt den Betrieb auf einer Vielzahl von Hardware- und Betriebssystem-Plattformen.

Systemadministration

Managed Objects
Nach automatischer Erkennung der Netzelemente in einer Netzdomäne kann ausgewählt werden, welche der Elemente durch HiPath FM überwacht werden sollen.
Die von HiPath FM zu überwachenden Netzelemente werden durch ausgewählte Attribute als Managed Objects im Server verwaltet. Die Verwaltung umfasst nicht nur die verschiedenen Netzknoten, sondern auch die Verbindungen zwischen diesen.

Benutzerverwaltung
Der Anwender-Zugriff auf die im Server gespeicherten Informationen ist durch Login und Password geschützt. Die grafische Benutzerverwaltung ermöglicht ein komfortables Einrichten, Modifizieren und Löschen von Benutzern.

Rechteverwaltung
Jedem Benutzer können abhängig von seinen Aufgaben individuelle Zugriffsrechte zugewiesen werden. Zur weiteren Vereinfachung sind 6 Benutzerprofile mit fest definierten Rechten vordefiniert.

7.7 TeleData Office V3.0

Kostenmanagement für Ihre Sprach- und Datenkommunikation

TeleData Office Version 3.0 ist in der Lage die Kommunikationsdaten an der technischen Quelle aufzuzeichnen oder über elektronischen Datenaustausch (Mobilfunk) einzulesen und deren Kosten zu berechnen. Die so entstehenden Kosten für Festnetz-, Internet- und Mobilkommunikation werden verursachergerecht aufgeschlüsselt.

Damit dies ohne Verwaltungsaufwand geschieht, lernt die Benutzerverwaltung von TeleData Office Version 3.0 alle Kommunikationsadressen selbst. Im Anschluss müssen die so erfassten Kommunikationsadressen nur noch einem Benutzer zugeordnet werden.

Damit schließt sich der Kreis: Durch den Einsatz professioneller Software sind auch im Internetzeitalter providerunabhängige Verbrauchsdatenerfassung und Transparenz bis in die kleinste Kostenstelle gesichert.

Corporate Communications Controlling

Controlling beginnt mit Kontrolle. Stimmt die Telefonrechnung? Wo entstehen die Kosten? Das betriebswirtschaftliche Management zielt daher auf Transparenz und eindeutige Zuordnung der Kosten auf den Verursacher. Gefragt ist neben den laufenden Betriebskosten die Dauer und der Zweck der Kommunikationsvorgänge. Denn auch die Zeit, die der Mitarbeiter für Kommunikation aufwendet, kostet Geld.

Die Leistungsfähigkeit der Kommunikationsinfrastruktur ist eine weitere Kostendimension. Jeder nötige Sprung zu höherer Bandbreite, weil die Netzlast erschöpft ist, bedeutet immer auch eine kräftige Investition in neue Hardware. Eine präzise Nutzungskontrolle dämpft den Migrationsdruck und spart Kosten.

8 Ausbaugrenzen und Kapazitäten

Erläuterungen der Tabelle:

Die genannten Anzahlen sind stets Maximalwerte.

N/A: nicht anwendbar, nicht zutreffend

.

Parameter	HiPath 2000
Agenten	
Agenten-IDs im System	
Gleichzeitig aktive Agenten im System	
Amtsberechtigung	
Anzahl der Erlaubnislisten im System	6
Anzahl der Verbotslisten im System	6
Erlaubnisliste kurz (10 Einträge à 32 Ziffern)	5
Erlaubnisliste lang (100 Einträge à 32 Ziffern)	1
Amtsberechtigung - Verbotsliste kurz, (10 Einträge à 32 Ziffern)	5
Verbotsliste lang (50 Einträge à 32 Ziffern)	5
Amtsleitungen	
Anzahl (B-Kanäle) im System	250
Anklopfen (wartende Anrufer)	
Anzahl wartender externer Anrufer pro Endgerät	5
Anzahl wartender interner Anrufer pro Endgerät	5
Anruferliste - von Endgeräten genutzt	
Anzahl der Einträge pro Liste	10
Anzahl der Listen im System	650
Anzahl der Listen pro Endgerät mit Anzeigefeld oder Teilnehmergruppe	1
Anzahl der Ziffern pro Eintrag	25 -stellige Rufnummer + Richtungs-Kennzahl
Anrufübernahmegruppen	
Anzahl der Teilnehmer einer Gruppe	32
Anzahl pro System	8

Parameter	HiPath 2000
Anrufumleitung (AUL)	
Alle Anrufe - gleichzeitig aktiv im System	500
Extern - Anzahl der AUL-Tasten pro Endgerät	as keys per telephone
Extern - Anzahl der Ziffern	25 -stellige Rufnummer + Richtungs-Kennzahl
Ansage automatisch	
Anzahl der Anrufer, denen gleichzeitig eine Ansage eingespielt werden kann	10
Ansagegeräte	
Anzahl der Endgeräte, denen gleichzeitig eine Ansage eingespielt werden kann	10
Anzahl im System	4
optiClient Attendant	
Anzahl der Halte-Tasten pro optiClient Attendant	4
Anzahl pro Gruppe	6
Gruppen im System	6
Überlauf - Anzahl der Anrufe in der Warteschlange	16
Anzahl der überwachten Nebenstellenanlagen pro Knoten für "Besetzt" -Überwachung	100
Berechtigungsklassen	
Anzahl im System	
Größe der Matrix- Tag und Nacht - Anzahl der Amtsleitungen	
Erlaubnis- und Verbotslisten	
Team/Top	
Anzahl der Führungskräfte (Chefs) mit persönlichen Assistenten pro Konfiguration	
Konfigurationen im System	10
PIN fürs Codeschloss/mobile PIN	
Anzahl der Ziffern des PIN-Codes	5
CSTA	
Anzahl der anschließbaren Applikationen pro System (Server)	8
Anzahl der gleichzeitigen Aufträge	64
Anzahl der TDS-Kennzahlen	

Parameter	HiPath 2000
Monitor Points	ab V2.0
Anzahl der CTI-Aufträge für CSTA Links	ab V2.0
DSS	
Beistellgeräte pro System	
Beistellgeräte pro Endgerät	
Anzahl der Tasten eines Beistellgeräts	
Anzahl der Tasten im Besetztlampenfeld (BLF)	90
Zahl der BLF im System	12
Durchwahlnummern	
Anzahl der Ziffern	11
Administration	
Zahl der gleichzeitigen Administratorzugriffe	1
Gesprächsdatenerfassung	
Anzahl der Einträge im Puffer	10.000
Ruftasten	
Anzahl der Ruftasten pro Endgerät	10
Gruppenruf	
Anzahl der Gruppen	10
Hotline/Hotline nach Zeitüberschreitung (Röchelschaltung (=code blue))	
Anzahl der Ziele	1
Konferenz	
Anzahl der Teilnehmer pro Konferenz	5
Anzahl der Konferenzen im System	6
Anzahl der Amtsverbindungen in einer Konferenz	4
Kurzwahl individuell (KWI)	
Anzahl der Einträge im System	
Anzahl der Einträge pro Endgerät	10
Anzahl der Ziffern pro Eintrag	25 -stellige Rufnummer + Richtungs-Kennzahl
Kurzwahl zentral (KWZ)	
Anzahl der Einträge im System	

Parameter	HiPath 2000
Anzahl der Ziffern pro Eintrag	25 -stellige Rufnummer + Richtungs-Kennzahl
Länge der Namen in Buchstaben	16
Leitweglenkung (LCR)	
Anzahl der gewählten Ziffern	32
Anzahl der überprüften Ziffern	25 -stellige Rufnummer + Richtungs-Kennzahl
Anzahl der Wahlpläne (à 10 Felder maximal)	514
Anzahl der Wahlregeln pro Richtung	254
Anzahl der Wege in einer Wegetabelle	16
Anzahl der Zeitzonen pro Tag/Woche	8
Anzahl der Ziffern pro Wahlregel	40
Leitungsvormerkungen (nicht S_0)	
Anzahl gleichzeitiger Einträge im System	N/A
MFV-Durchwahl	
Anzahl gleichzeitiger Vorgänge	N/A
MULAP-Tasten	
Zahl der Tasten eines Endgeräts	
Nachrichtentexte	
Anzahl der Abwesenheitstexte im System	250
Anzahl empfangener Nachrichten bei einem Endgerät mit Anzeigefeld (+1 für Voice Mail)	5+1
Anzahl der Infotexte im System	150
Anzahl empfangener Nachrichten bei einem Endgerät mit Anzeigefeld (+1 für Voice Mail)	1+1
konfigurierbare (Infotexte + Abwesenheitstexte) im System	10+10
Länge des Textes bei einer kundendefinierten Nachricht in Wörtern	24
Länge des Textes einer generierten Nachricht in Wörtern	24
Mailbox: Anzahl der gleichzeitig aktiven Nachrichten im System (Infotexte + Abwesenheitstexte)	250
Namensanzeige	
Für interne Teilnehmer und Teilnehmergruppen - Länge in Buchstaben	16

Parameter	HiPath 2000
KWZ - Länge in Buchstaben	16
Richtungen: Länge in Buchstaben	10
Teilnehmer (Endgeräte)	
Anzahl der Teilnehmer (erweitert)	
Parkpositionen	
Anzahl im System	Up to 11
Projektkennzahl	
Anzahl prüfbarer Ziffern	11
Anzahl im System	1000
Richtungen	
Anzahl in System	16
Richtungsüberlauf	
Anzahl pro Richtung	1
Rückruf	
Anzahl der Einträge pro Amtsleitung	64
Anzahl der Einträge pro Teilnehmer (jeweils gesendete und empfangene pro Nebenstelle))	5
Rufweiterschaltung (RWS) (wird im Call Management fest konfiguriert)	
Im Frei- oder Besetztfall: Anzahl pro Endgerät	1
Anzahl der RWS-Ziele pro Teilnehmer	1+3
Anzahl der Ziele in der Call Management Liste	500
CFSS Ziele pro System	250
Anrufübernahmegruppen (konfigurierbar)	
Anzahl der Nebenstellen	5
Sprachen	
Anzahl der im System gleichzeitig aktiven Sprachen (fest vorgegeben+frei installierbar))	
Teilnehmergruppen	
Länge der Gruppennamen	16
Anzahl der Endgeräte pro Gruppe	20 (24)
Anzahl der Gruppen für den Gruppenruf, Sammelanschluss, MULAPs, Durchsagezonen	800

Parameter	HiPath 2000
Anzahl der Anschlüsse pro Gruppe mit Voice Mail Support (nur ein Sammelanschluss pro System)	20 (24)
Teilnehmerrufnummern	
Gesamtanzahl im System (einschließlich Teilnehmer- und Gruppenrufnummern)	
Anzahl der Nebenstellen-Rufnummern im System	
Anzahl der Gruppen- und Sammelanschluss-Rufnummern im System	800
Maximale Länge der Rufnummer	6
Länge der Rufnummer (Voreinstellung)	3
Telefonbuch intern	
Anzahl gleichzeitiger Zugriffe (praktisch unbegrenzt)	alle Geräte mit Anzeigefeld
Telefonbuch extern (LDAP)	
LDAP Verzeichnis: Anzahl gleichzeitiger Zugriffe	20
Türöffner	
Anzahl ungültiger Kennworteingabeversuche vor einer Deaktivierung	5
Ziffernanzahl der PIN	5
Universal Call Distribution (UCD)	
Anzahl der Prioritätsebenen pro Anruftyp	10
Anzahl der Ansagen pro Gruppe	7
Anzahl der Gruppen im System	
Anzahl wartender Anrufe pro Gruppe	30
Vernetzung	
Anzahl der Richtungskennzahlen	10
Anzahl der Ziffern einer Richtungskennzahl	6
Wahlwiederholung (LNR)	
Anzahl der Einträge eines Endgeräts mit Anzeigefeld	3
Anzahl der Einträge eines Endgeräts ohne Anzeigefeld	1
Anzahl der gespeicherten Ziffern	25 -stellige Rufnummer + Richtungs-Kennzahl
Wartemusik	

Parameter	HiPath 2000
Anzahl externer Verbindungen	6
Zieltaste / KWI	
Anzahl der Ziele im System	
Anzahl der Ziffern pro Ziel	25 -stellige Rufnummer + Richtungs-Kennzahl
Tenant System (siehe unten: Fax-und Modem-Rufnummern)	
Tenants pro System	1
VBZ-Gruppen	
Anzahl der VBZ-Gruppen	6
Anzahl der vom Administrator einzurichtenden Fax- und Modem-Rufnummern (pro Knoten)	
Location identification number (LIN), USA only	
Anzahl der Ziffern	11

Tabellen

Stichwörter

Abkürzungen

Diese Liste enthält die in diesem Handbuch verwendeten Abkürzungen.

Abkürzung	Definition
A	
APS	Anlagenprogrammsystem
AES	Advanced Encryption Standard
B	
BHCA	Busy Hour Call Attempts
BSG	Beistellgerät
BOOTP	Bootstrap Protocol
C	
CCBS	Completition of Calls to Busy Subscribers
CDB	Customer Database
CLA	Customer License Agent
CLC	Customer License Client
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CLM	Customer License Manager
CLS	Central License Server
D	
DHCP	Dynamic Host Configuration Protocol
DMC	Direct Media Connection
DMZ	Demilitarized Zone
DSP	Digital Signal Processor
E	
EGB	Elektrostatisch Gefährdete Bauelemente
EVM	Entry Voice Mail
G	
GAP	Generic Access Profile

Abkürzung	Definition
GPCF	Grace Period Configuration File
I	
IP	Internet Protocol
K	
KDS	Kundendatenspeicher
L	
LAC	License Authorization Code
LAN	Local Area network
LH	License Handler
LDAP	Lightweight Directory Access Protocoll
LED	Light Emitting Diode
LM	Leistungsmerkmal
M	
MOH	Music On Hold
MSN	Multiple Subscriber Number
MW	Mini Western
N	
NT	Network Termination
P	
PCM	Pulse Code Modulation
PRI	Primary Rate Interface PRI
PPPOE	Point to Point Protocol Over Ethernet
PPTP	Point to Point Tunneling Protocol
Q	
QDC	QoS Data Collection
QoS	Quality of Service
R	
RJ	Registered Jack
RLF	Real License File
RSA	Resilience Service Application
RSM	Real-Time Services Manager

Abkürzung	Definition
S	
SELV	Safety Extra-Low Voltage Circuit
SIP	Session Initiation Protocol
SMR	Service Maintenance Release
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SNG	Steckernetzgerät
SP	Service Provider
SSL	Secure Socket Layer
T	
TAPI	Telephony Application Programming Interface
U	
USB	Universal Serial Bus
V	
VPN	Virtual Private Network
W	
WAN	Wide Area Network
WAP	Wireless Application Protocol
WBM	Web-based Management
WLAN	Wireless LAN
WP	Workpoint